Oili Koivuharju

Tietoturva järjestelmäkehityksessä

Metropolia Ammattikorkeakoulu

Ylempi Ammattikorkeakoulututkinto (YAMK)

Yrittäjyyden ja liiketoimintaosaamisen koulutusohjelma

Opinnäytetyö

29.10.2013

Metropolia

Tekijä Otsikko Sivumäärä Aika	Oili Koivuharju Tietoturva järjestelmäkehityksessä 68 sivua + 5 liitettä 29.10.2013
Tutkinto	Ylempi ammattikorkeakoulututkinto
Koulutusohjelma	Yrittäjyys ja liiketoimintaosaamisen koulutusohjelma
Suuntautumisvaihtoehto	Tietohallintojohtaminen
Ohjaaja	Lehtori Erkki Sairanen

Liiketoiminnan kannalta kriittisen tiedon suojaaminen ja turvaaminen on yritysten menestyksellisen toiminnan ja sen jatkuvuuden kannalta tärkeää. Tietoturvan hallinnan avulla pyritään varmistamaan tiedon eheys, luottamuksellisuus ja käytettävyys sekä kiistämättömyys, todentaminen ja pääsynvalvonta.

Tutkimuksen tavoitteena oli selvittää ne tietoturvan kohdat, joissa tarvitaan selkiyttämistä ja lisää ohjeistusta käytettäessä uutta iteratiivista systeemityömenetelmää.

Tutkimus oli luonteeltaan kvalitatiivinen toimintatutkimus, jossa teorioita sovellettiin Kelan tapaukseen.

Työn teoriaosuudessa on selvitetty ja esitelty tietoturvan keskeisiä peruskäsitteitä, periaatteita, IT-riskienhallintaa tietoturvan näkökulmasta sekä käytettyjä tietoturvastandardeja ja ohjeita.

Tutkimuksen tuloksena on saatu aikaan tietoturvaohjeistus, jossa tietoturvatehtävien jaottelussa on huomioitu systeemityömenetelmän eri elinkaarivaiheet.

Tulokset on koottu opinnäytetyön loppuun eri liitteeksi.

Avainsanat	tietoturva, tietoturvan hallinta, tietoturvariskien hallinta, elinkaarivaiheet

Author	Oili Koivuharju
Title	Information Security in Software Development
Number of Pages	68 pages + 5 appendices
Date	29 Oct 2013
Degree	Master of Business Administration
Degree Programme	Entrepreneurship and Business Competence
Specialisation option	Business Information Management
Instructor	Erkki Sairanen, Senior lecturer

Protecting and securing the business-critical information is important in order to maintain successful operation and its continuity. Information security management ensures the integrity, confidentiality and availability also non-repudiation, authentication of information and access control.

The aim of this research was to clarify such cases of data security where more knowledge and instructions is needed in when new iterative software development process is used.

The research was qualitative case study in which the theoretical part was adapted in Kela.

In the theory section of the thesis, the reader is introduced to a general terms of information security, information security basics, information security risk management in the point of view of information security and also used information security standards and guidelines.

The result of this research is an information security instructions where different life cycles of software development process has been noticed in information security task based grouping.

The results are compiled in annexes at the end of this thesis.

Keywords	Information Security, Information Security Management, Information Security Risk Management, Life cycles of System Development

Sisällys

Termistö

Termi	Kuvaus
COSO-ERM	Kokonaisvaltainen sisäisen valvonnan ja riskienhallinnan malli.
Eheys	Tiedot ja tietojärjestelmät ovat luotettavia, oikeellisia ja ajantasaisia, eivätkä ne ole hallitsemattomasti muuttuneet tai muutettavissa laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena (aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus).
Elinkaarivaihe	Aika järjestelmän syntymisestä sen loppumiseen tai käytöstä poistamiseen.
Inkrementaalinen (kasvattava)	Iteraatioissa valmistuu elinkaaren aikana valmiita osia rakenteilla olevasta järjestelmästä.
Iteratiivinen (kehittävä)	Samoja työvaiheita toistetaan järjestelmäkehityksen elinkaarivaiheiden aikana.
Kiistämättömyys	Tietojärjestelmä pystyy luotettavasti tunnistamaan ja tallentamaan järjestelmän käyttäjän tiedot sekä tietojärjestelmässä tapahtuneet toimenpiteet.
Käytettävyys	Järjestelmien tiedot tai palvelut ovat niihin oikeutetuille käyttäjille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.
Luottamuksellisuus	Tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen käytettävissä eikä sivullisille anneta mahdollisuutta muuttaa tai tuhota tietoja, eikä muutoin käsitellä tietoja eikä niitä paljasteta tai muutoin saateta sivullisten käyttöön.
Pääsynvalvonta	Toiminnot ja menettelyt, joiden avulla tietojärjestelmään pääsy tai tiedon saanti sallitaan vain valtuutetuille henkilöille tai sovelluksille (ohjelmat, prosessi tai muut järjestelmät).
Riski	Todennäköisyys, että uhka toteutuu aiheuttaen tietyn menetyksen tai vahingon.
Riskianalyysi	Systemaattisin menetelmin tapahtuva uhkien ja riskien arviointi.
RUP	IBMn Rational Unified Process on iteratiivinen ohjelmistokehityksen prosessimalli, jossa työ perustuu erikseen hallinnoitaviin työpaketteihin.
Systeemityömenetelmä	Joukko menettelytapoja ja ohjeita, joiden mukaisesti tietojärjestelmien kehittäminen, ylläpito ja käytöstä poisto tehdään.
Tietojärjestelmä	Tietokonelaitteista (tietovälineet, muistit, tulostimet, lukulaitteet), tietoliikenneyhteyksien (kaapelit, verkkolaitteet, palvelut) ja ohjelmistoista (käyttöjärjestelmä, sovellukset, apuohjelmat) koostuva kokonaisuus, jolla käsitellään dataa (teksti, kuva, ääni) järjestelmälle määriteltyjen toimintojen ja sääntöjen mukaisesti ja jonka tavoitteena on tehostaa tai helpottaa jotain toimintaa tai tehdä toiminta mahdolliseksi.
Tietoturvan hallintajärjestelmä	Prosessi ja menettelytavat, joilla organisaation tietoturvallisuustoimintaa perustetaan, ja joilla sitä ylläpidetään, seurataan, kehitetään ja mitataan. Sen avulla organisaation johto saa tietoa tietoturvan tasosta ja jonka avulla toimintaa ohjataan haluttuun suuntaan.
Tietoturva	Tietojen, tietojärjestelmien, laitteiden, palveluiden sekä tietoliikenteen suojaamista hallinnollisilla, teknisillä tai muilla toimenpiteillä erilaisia uhkia vastaan siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu.
Tietoturvapolitiikka	Organisaation ylimmän johdon hyväksymä näkemys ja julkaistu kannanotto tietoturvallisuuden päämääristä, periaatteista ja toteutuksista.

1 Johdanto

1.1 Yleistä

Tietoturvallisuus on osa jokaisen organisaation liiketoimintaa ja riskienhallintaa. Toiminnan jatkuvuus ja laadukas toiminta edellyttää asiallisesti hoidettua tietoturvallisuutta. Tietoturva-asioiden oikeanlainen hoitaminen voi olla edellytyksenä sopimuksen tai liikekumppanuuden syntymiselle. Myös yrityksen maine ja yrityskuva sekä luottamus palveluun ovat tärkeitä tekijöitä sen liiketoiminnan kannalta.

Tietoturvallisuuden merkitystä korostavat asetetut lakisääteiset velvoitteet, tietoturvallisuushyökkäysten ja muiden uhkien lisääntyminen, nopeutuva tietoyhteiskuntakehitys, sähköisen asioinnin lisääntyminen, kansainvälistyminen, organisaatioiden verkottuminen, tietotekniikka- ja verkkopalvelusektorin (ICT) nopea tekninen kehitys sekä toimintojen ja palveluiden siirtyminen tietoverkkoihin. (VAHTI 3/2003, 7.)

Tietoturvallisuuden riittävä taso on välttämätön edellytys toiminnan jatkuvuudelle ja uskottavuudelle. Tietoturvallisuus parantaa organisaation toiminnan tehokkuutta ja laatua. Tietoturvallisuuden avulla taataan organisaatiossa käsiteltävän tiedon eheys, käytettävyys ja luottamuksellisuus. (VAHTI 2/2004, 5.)

Hyvä tietoturvakulttuuri muodostuu hyvästä johtamisesta, johtajien luomista arvoista ja tietoturvatietoisuuden lisäämisestä. Vaikka vastuu tietoturvallisuudesta huolehtimisesta on organisaation johdolla, niin jokainen organisaation jäsen vaikuttaa siihen omalla toiminnallaan.

Tietoturvalla tavoitellaan tiedon käsittelyyn liittyvien turvallisuusvaatimusten hallittuun toteuttamiseen kaikissa käsittelyn vaiheissa. Tietoturvallisuuden hallinnan tulee ottaa huomioon:

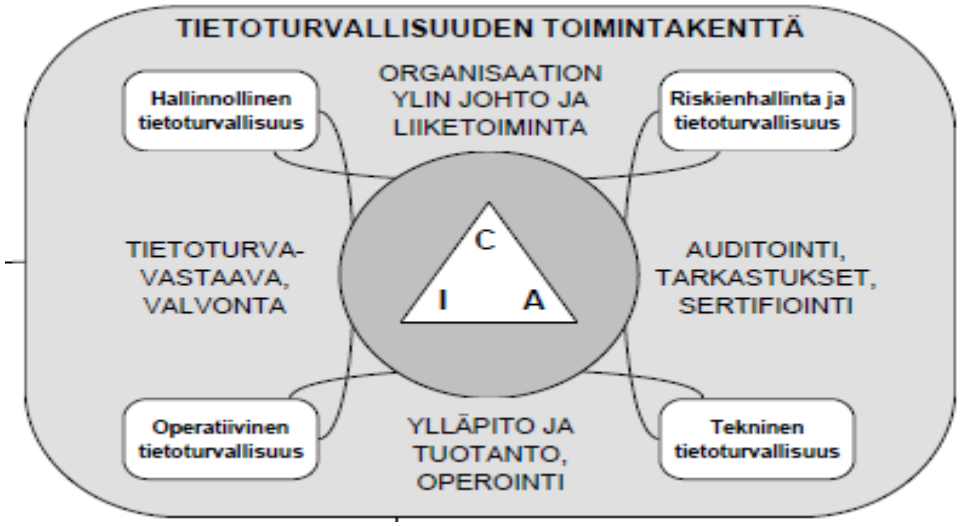
- Tiedon eri esiintymismuodot (päässä, paperilla, puhuttu, tallenne, tietojärjestelmä)
- Tiedon käsittelytavat (lukeminen, siirtäminen, puhuminen, poistaminen, muuttaminen, kopioiminen)
- Tietoon kohdistuvat riskit ja turvaamisen toteuttamisen keinot

- Toimintaan ja sitä kautta tietoon kohdistuvat vaatimukset. (Valtionhallinnon tietoturvatasot – esitutkimus 2007, 7.)

Tietoturvanäkökulma tulee olla mukana tietojärjestelmän elinkaaren kaikissa työvaiheissa alkaen esiselvityksestä päätyen tietojärjestelmän käytöstä poistamiseen. Riippumatta siitä millä menetelmällä tietojärjestelmä on kehitetty, on samat turvatoimet otettava huomioon. Tietojärjestelmä kehitetään palveluina, moduuleina tai komponentteina, jotka sitten integroidaan toimintaympäristöön. Kehittämisen tavoitteena on saada aikaan halutut vaikutukset tuottava toiminta. (Huhanantti, 14.)

Tietoturvallisuuden kehittäminen ja ylläpito on jatkuvaa toimintaa, joka tapahtuu hallinnollisten, fyysisten ja tietoteknisten ratkaisujen avulla.

Tietoturvallisuuden toimintakentän kokonaisuutta on hahmotettu kuviossa 1.



Kuvio 1. Tietoturvallisuuden toimintakenttä. (Kangas 2010, jakso 3, 22.)

1.2 Kohdeorganisaation kuvaus

Kohdeorganisaationa oleva Kansaneläkelaitos (Kela) perustettiin vuonna 1937. Kela on itsenäinen julkisoikeudellinen laitos, jonka hallintoa ja toimintaa valvovat eduskunnan valitsemat valtuutetut. Kela huolehtii Suomessa asuvien perusturvasta eri elämäntilanteissa.

Kela on luotettava, tehokas ja sosiaalisen vastuunsa tunteva toimija. Lisäksi se on aktiivinen sosiaaliturvan ja sen toimeenpanon kehittäjä. Kelasta saatava sosiaaliturva on tasoltaan kohtuullista, laadukasta ja selkeää.

Kelan toimintaa ohjaavat useat lait, asetukset ja ohjeet. Tällaisia ovat mm. henkilötietolaki (523/1999), laki viranomaisten toiminnan julkisuudesta (621/1999), sähköisen viestinnän tietosuojalaki (516/2004) sekä Kelan toimeenpanemien etuuslakien tietojen saamista ja luovuttamista koskevat säännökset. Useat lait ja asetukset sisältävät Kelaa koskevia tietoturvallisuusvelvoitteita. Niihin sisältyy tietosuojaa, hyvää tiedonhallintatapaa ja tietoturvallisuutta koskevia velvoitteita. Lait velvoittavat Kelaa huolehtimaan tietojen luottamuksellisuudesta, eheydestä ja käytettävyydestä.

Kelan palveluverkossa on toimistoja ja yhteispalvelupisteitä yli 300 ja henkilöstön määrä on noin 6 000. Vuosittain Kelassa ratkaistaan yli neljä miljoonaa etuushakemusta. Vuonna 2012 Kelan verkkosivuilla käytiin 18,9 miljoonaa kertaa (v.2011 16,3 milj.).

Tutkimuksen aihe on ajankohtainen toimeksiantajalle. Kehittämistehtävä laaditaan Kelan Tietohallinto-osaston tietohallintoryhmälle. Tietohallintoryhmän vuoden 2011 tulossopimukseen on kirjattu prosessien parantamiseen tähtääviä kehittämiskohteita ja tietoturvaan liittyvänä on: Tietoturvan ylläpito, kehittäminen ja jatkuvuuden suunnittelu. Tämä kehittämistehtävä on yksi tähän liittyvä kohde.

2 Tutkimusasetelma

Tämän kehittämistehtävän tavoitteena on esitutkimusvaiheessa selvittää järjestelmäkehittämisen elinkaarivaiheiden tietoturvatehtäviä Kelassa ja laatia kootusta kokonaisuudesta tietoturvaohjeistus, jota noudattamalla tietoturvatehtävien huomioiminen varmistuu järjestelmäkehittämisen elinkaaren eri vaiheissa. Tutkimus on työelämälähtöinen kehittämisongelma, jolle on Kelassa selkeä tarve. Tutkimuksessa keskitytään Kelan tietoturvallisuuteen iteratiivisen ja inkrementaalisen tietojärjestelmän kehittämisen näkökulmasta.

Esitutkimusvaiheessa laaditaan kuvaus tietoturvaprosessista tietojärjestelmien näkökulmasta ja siihen liittyvä seliteteksti.

Haastatteluiden ja kyselyn avulla selvitän järjestelmäkehityksen tietoturvan tilaa sekä toimihenkilöiden näkemystä tarvittavasta tietoturvaohjeistuksesta.

Kehittämistehtävän oppimistavoitteina on tutkivan ja kehittävän työotteen omaksuminen sekä arvioida kriittisesti valittujen kehittämismenetelmien soveltuvuutta ja tuotettujen lopputulosten toimivuutta. Kehittämistehtävässä on tärkeää kytkentä tosiasiallisiin kehittämistarpeisiin sekä yhteys teoriaan. Tärkeätä on myös se, että työyhteisön asianosaiset osallistuvat kehittämistehtävän eri vaiheisiin.

2.1 Tutkimuskysymykset

Kehittämistehtävän avulla haetaan vastausta seuraaviin tutkimuskysymyksiin:

1. Miten tietoturva liittyy tietojärjestelmäkehityksen eri elinkaarivaiheisiin ja millaisia tietoturvatehtäviä tunnistetaan?

2. Mitkä tietoturvan osa-alueet on koettu ongelmallisiksi tietojärjestelmän kehittämisessä, joihin tarvitaan henkilöstön tietoturvatietämyksen lisäämistä järjestelmäkehityksessä?

3. Miten käytännön tietoturvaohjeita tulisi kehittää vastaamaan paremmin käyttäjien tarpeita?

2.2 Rajaus

Kehittämistyöstä rajataan pois systeemityön kehitysvaiheen jälkeiset vaiheet eli käytön aikainen tietoturva, ylläpitoon, järjestelmän käytöstä poistoon sekä arkistointivaatimuksiin liittyvät osuudet. Tietoturvahallintaan liittyviä asioita ei käsitellä tarkasti.

Kehittämistehtävän lopputuloksien esittelyyn ja implementointiin liittyvien asioiden käsittely rajataan myös tämän tutkimustyön vaiheista.

3 Menetelmät

Tässä luvussa esitellään kehittämistehtävässä käytetty tutkimusmenetelmä sekä tiedon keräämisen tavat.

3.1 Tutkimusmenetelmät

Työelämälähtöisen kehittämistehtävän tutkimusmenetelmä on toimintatutkimus, jossa pyritään kehittämään olemassa olevaa käytäntöä paremmaksi. Tutkijana osallistun itse aktiivisesti toiminnan kehittämiseen ja pyrimme yhdessä toimeksiantajan kanssa parantamaan kehitettävää kohdetta. Empiriaosuudessa käytetään tiedon keruun menetelminä myös henkilökohtaisia haastatteluja ja kyselyä.

Toimintatutkimuksen aineiston käsittelyn metodologiana käytetään kvalitatiivista eli laadullista tutkimusmenetelmää. Tutkimuksessa korostuu käytännön ja teorian vuorovaikutuksellinen suhde. Tutkimuksessa halutaan saada selville käyttäjien kokemuksia ja heidän arvionsa käytössä olevien tietoturvaohjeiden käytettävyydestä ja laadusta. Tutkimukseen osallistuva kohdejoukko valitaan tarkoituksenmukaisesti.

Haastatteluilla kerätään tietoa dokumentoinnin nykytilasta sekä tahtotilasta. Kirjallisuuden avulla selvitetään tietoturvallisuuden pääperiaatteita ja erilaisia menettelytapoja sekä tietoturvallisuuden arviointiin liittyviä asioita tietojärjestelmäprojektin elinkaaren eri työvaiheissa. Haastateltavaksi valitaan henkilöitä, joilla on kokemusta tietoturvaasioista. Haastateltujen ohessa kartoitan mitä tietoturvaan liittyviä systeemityön ohjeita on nykyisin käytössä ja minkälaista ohjeistusta olisi hyvä olla tarjolla.

3.2 Tiedon kerääminen

Toimintatutkimusta varten kerätään ensimmäiseksi materiaali teoreettista taustaa varten. Materiaalia koostan tutustumalla alan ja työn aiheeseen liittyvään kirjallisuuteen sekä lehtiartikkeleihin. Apuna käytän myös luotettavia sähköisiä tietoverkkoja sekä opintomateriaaleja.

Kehittämistehtävä jakautuu kahteen vaiheeseen. Ensimmäisessä vaiheessa kartoitetaan nykytilanne ja kerätään tutkimusaineistoa kirjallisella kyselyllä. Kyselyn avulla pyri-

tään selvittämään henkilöstön tietoturvaohjeistuksien lisätarvetta. Saaduista vastauksista laaditaan yhteenveto. Vastauksien sisältöä käytetään laadittavaan uuteen ohjeistukseen. Kysely toteutetaan sähköpostilla. Kyselyn vastaajiksi pyritään valitsemaan henkilöt joiden osa-alueelle uuden systeemityömenetelmän tehtävät kuuluvat.

Toiseksi tavoitteeksi tuli se, että laadittaisiin prosessikartta, joka kuvaa tietoturvaprosessia tietojärjestelmien näkökulmasta.

Toisessa vaiheen tehtävät määrittyvät nykytilasta. Tehtävien kokonaissisällön tarvetta ja asiasisältöä pohditaan työpajoissa. Ko. tilaisuuksiin pyydetään ao. alueen asiantuntijoita. Työvaiheisiin kuuluu vielä reflektoiva kysely, jossa valitut henkilöt arvioivat ohjeistuksen hyödyllisyyttä omaan työtehtäväänsä nähden.

3.3 Mittarit

3.3.1 Yleistä mittareista

Tässä luvussa käsitellään hieman mittareista yleensä sekä Kelalle tietoturvaan kehittämistehtävän aikana suunnitellut mittarit.

Mitattavuus tulee huomioida jo tietojärjestelmiä kehitettäessä tai hankittaessa. Mittaustulosten raportointimenettelyt tulee myös suunnitella. (VAHTI 5/2004, 96.)

Mittarin tärkeimmät ominaisuudet ovat luotettavuus, soveltuvuus, yksiselitteisyys, helppolukuisuus, oikea-aikaisuus ja olennaisuus. (Loula 2008, 66.)

Tietoturvatoiminnan mittaus on osa johtamisen ja tietoturvallisuuden hallintaprosessia. Jotta mittaamisesta muodostuisi jatkuvaa toimintaa ja aikaansaataisiin aikasarjoja, on käytettävän mittariston oltava riittävän selkeä. Mittareita tulee olla mieluummin vähän ja kuvaavia sekä ohjaavia, kuin paljon ja kaiken kattavia.

Tietoturvatason toteutumista voidaan seurata pysyväisluontoisilla mittareilla. Yleisimpiä seurantakohteita ovat tietoturvapoikkeamat ja tietoturvatoiminta sekä niissä tapahtuneet muutokset. Näillä mitataan absoluuttisia arvoja ja siten voidaan seurata tietoturvatason kehittymistä. (VAHTI 6/2006, 34.)

Tapahtuneissa tietoturvapoikkeamissa seurataan ja mitataan toiminnalle aiheutuvaa haittaa ja hankitaan tietoa tietoturvatoimenpiteiden suunnittelua varten. Mittareita ovat mm. ilmoitetut/tietoon tulleet toimenpiteitä vaatineiden tietoturvatapahtumien lukumäärä, raportoitujen tietoturvarikkomusten luonne ja määrä, virus- ja muut haittaohjelmavahingot ja torjuntaprosentti ja verkon poikkeukselliset kuormitustilanteet. (VAHTI 6/2006, 35.)

Tietoturvatoimintaa kuvaavissa mittareissa arvioidaan tietoturvatoiminnan tehokkuutta seuraamalla suoritteita ja käytettyjä panoksia. Mittareita ovat mm. tietoturvatoiminnan kustannukset (kehittäminen, operatiivinen toiminta, investoinnit) ja tietoturvallisuustyön työtunnit tai henkilötyöpäivät ja tietoturvaryhmän kokousten lukumäärä. (VAHTI 6/2006, 35.)

Mittareiden oikeanlaisuus vaatii jatkuvaa arviointia ja kehittämistä, jotta niiden hyödyllisyys ja tarkoituksenmukaisuus on varmistettu. Tietoturvallisuuden toimintaympäristössä tapahtuvat muutokset edellyttävät mittarien ja arviointimenetelmien jatkuvaa ajantasaistamista. (VAHTI 6/2006, 36.)

Tietoturvatason mittauksen seurannassa voidaan käyttää joko laadullisia (kvalitatiivisia) tai määrällisiä (kvantitatiivisia) mittareita.

3.3.2 Kvalitatiiviset mittarit

Laadullisessa mittaamisessa arvioidaan toiminnan onnistumista ja se on sopiva toiminnan tilan ja siinä tapahtuneen kehityksen arviointiin. (VAHTI 6/2006, 32.)

Laadullisia mittareita ovat mm.

- henkilöstön tietoturvallisuustietoisuuden arviointi
- riskien aiheuttamien uhkien seurausten arviointi
- tietoturvallisuuteen liittyvien ohjeiden ja koulutuksen arviointi. (Loula 2008, 66.)

3.3.3 Kvantitatiiviset mittarit

Määrällisessä mittaamisessa seurataan esimerkiksi tulosten aikaansaamiseen käytettyä työaikaa, kustannuksia, työajan menetystä, tietoturvapoikkeamien lukumääriä tai tietoturvakoulutuksien määriä. (VAHTI 6/2006, 32-33.)

Määrällisiä mittareita ovat mm.

- teknisten asioiden mittaamiseen – esim. luvattomat tunkeutumisyritykset tietojärjestelmiin
- toiminnan kustannusten mittaamiseen – väärinkäytön tutkinnan ja korjaamisen aiheuttamat kustannukset. (Miettinen 1999, 111.)

3.3.4 Kehittämistehtävään liittyvät mittarit

Oheiseen taulukkoon (1) on kirjattu mittarit, jotka jalostuivat Kelan tietoturvaan liittyviksi mittareiksi tämän kehittämistehtävän aikana.

Taulukko 1. Tietoturvan arvioinnin mittarit.

Mittari	**Selitys/Kuvaus**	**Toteutus**	**Kaava, yksikkö**	**Tavoite**	**2012**	**2013**
Laadullinen						
Käyttäjätyytyväisyys	Käyttäjäpalautteen keruu ja analysointi Tietoturvaohjeistuksen toimivuus ja parantamisen kehitys. Tavoitteena on varmistaa kohdentuuko tietoturvatoimenpiteisiin liittyvät ohjeistukset oikein Mittaa ohjeiden käyttäjien tyytyväisyyttä palveluun tai palvelukokonaisuuteen.	Tyytyväisyysmittaus kyselynä	Palautteen pisteistä keskiarvo. Palautteen keskiarvon suhde tavoitekeskiarvoon (%)			
Luotettavuus	Tietoturvakyselyn palautusprosentti	Tyytyväisyysmittaus kysely	Lähetettyjen kyselyjen määrä / palautetut (%)			
Tietoturvan toimintavarmuus	Tietoturvan toimivuus	Hälytysjärjestelmän kehitys /Tietoturvapalvelun yhteisten tietoturvapalvelujen käyttökatkot	Keskiarvo katkoista ajassa per palvelu % kokonaisaika			
Määrällinen						
Kulunut työaika	Ongelman ratkaisuun kulunut työaikaa	Työajankäytön seurannan raportti	h			
Poikkeamien määrä	Toimenpiteitä vaatineiden tietoturvapoikkeamien lukumäärä	Kerätään havaintokorteilta lkm:t	kpl			

4 Johdatus tietoturva ajatteluun

Tässä luvussa käsitellään tietoturvallisuuteen liittyviä keskeisiä peruskäsitteitä, jotka ovat keskeisiä kehittämistehtävässä. Lisäksi tarkastellaan hieman IT-riskienhallintaa sekä lainsäädännöllisiä vaatimuksia.

Valtionvarainministeriön VAHTI-julkaisu (5/2003, 8.) määrittelee tietoturvan seuraavasti: ”Tietoturvallisuudella tarkoitetaan tietojen, järjestelmin, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietoturvallisuuden tavoitteena on tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaaminen laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta.”

Tietoturvallisuus on tehokkaiden sovellusten toteuttamiseksi sekä lainsäädännöllisten ja muiden normien velvoitteiden täyttämiseksi välttämätöntä.

Tietoturvallisuus ja sen tuloksekas johtaminen edellyttää johdon sitoutumista tietoturvallisuuden kehittämiseen. Tietoturvallisuuden johtamisen perustana on ajantasainen tietoturvapolitiikka. Tietoturvapolitiikan avulla liikkeenjohto osoittaa sitoutumisensa ja tukensa turvallisuuden kehittämiseen. (Laaksonen & Nevasalo & Tomula 2006, 146.)

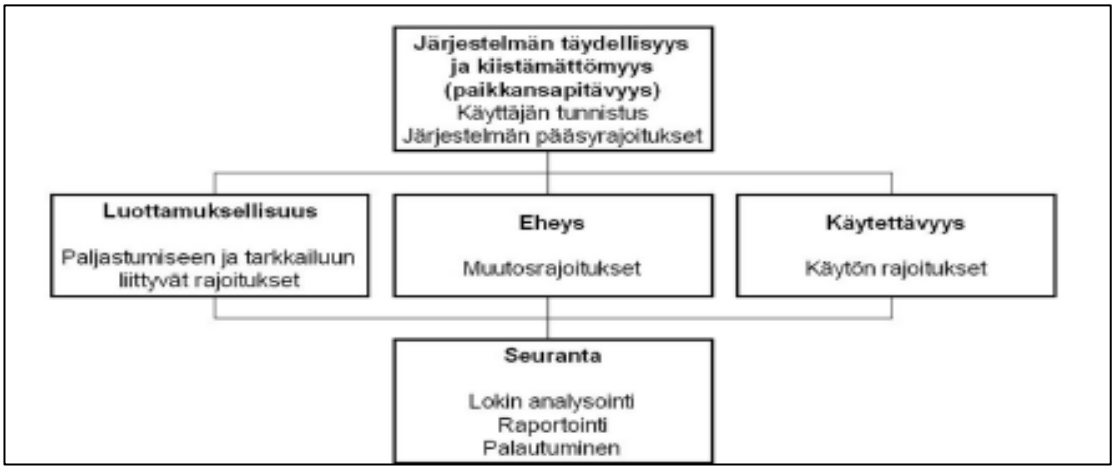
4.1 Tiedon määritystä

Valtionvarainministeriön VAHTI-julkaisu (5/2003, 11.) määrittelee tiedon seuraavasti ”Tiedolla tarkoitetaan eri muodoissa talletettavaa, käsiteltävää tai siirrettävää tietoa. Tieto voi olla yksittäisenä asiakirjana, tiedostona, ääni- tai kuvanauhana, puheena, tietokantana, suoritettavana ohjelmana, näytteenä tai muussa muodossa. Tiedon käsittelyvaiheet ovat luominen, käyttäminen, muuttaminen, tallettaminen, siirtäminen, jakelu, kopioiminen, arkistointi sekä poistaminen. Käsiteltävät tiedot ovat usein merkittävästi arvokkaampia kuin tietojen käsittelyssä käytettävä väline ja siksi tietoja on suojattava kaikissa sen käsittelyvaiheissa. Tietoa on tarkasteltava tiedon koko elinkaaren ajalta.

4.2 Tiedon merkitys toiminnalle

Tietoturvan avulla suojataan tietoa, tietojärjestelmiä ja palveluja niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvilta uhilta. Tietoturvaan kuuluu myös lainsäädäntö ja ne toimenpiteet, joiden avulla tietoturva varmistetaan.

Tietoturvatoiminnan tavoitteena on varmistaa luottamuksellisuus, eheys ja saatavuus. Sen lisäksi tarvitaan kiistämättömyyttä silloin kun tietojärjestelmän käytössä tehtyjen tapahtumien todentaminen ja niiden tekijöiden paikkansa pitävyys on tärkeää. (Teollisuusautomaation tietoturva, 28.). Kuviossa 2 on kuvattu tietoturvatoiminnan tavoitteita.



Kuvio 2. Tietoturvatoiminnan tavoitteet (Teollisuusautomaation tietoturva 2005, 28.)

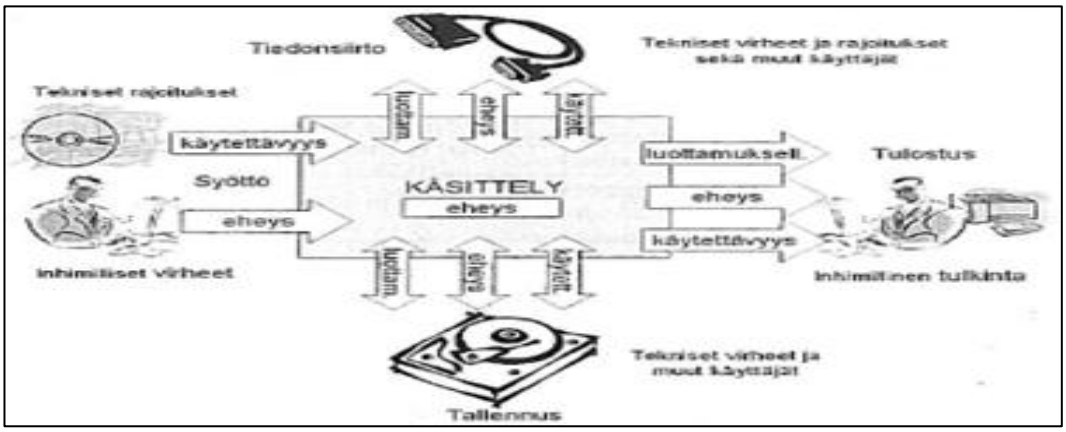
Tietoturvallisuudella tähdätään tiedon käsittelyyn kohdistuvien turvallisuusvaatimusten hallittuun toteuttamiseen kaikissa käsittelyn vaiheissa. Tämä tarkoittaa, että turvatoimenpiteet ja –menettelyt ovat suunniteltuja, laadukkaita sekä perusteltuja.

4.3 Tietoturvan peruselementit

Ohessa on esitelty tämän kehittämistehtävän keskeisimmät tietoturvallisuustoiminnan peruskäsitteet, jotka on koostettu eri lähteistä. Ko. käsitteiden määritys ei ole vakiintunutta. Olen kirjannut ko. määrityksistä kehittämistehtävän kannalta sopivassa laajuudessa ja joissain kohdin laajentanut kirjaviittauksen määritystä.

Tietoturva muodostetaan yleensä seuraavista keskeisistä käsitteistä: luottamuksellisuus (confidentiality), eheys (integrity) sekä käytettävyys/saatavuus (availability). Kuitenkin edellä mainittujen peruskäsitteiden lisäksi tietoturva edellyttää kolmen muun periaatteen toteutumista, jotka ovat todentaminen (authentication), pääsynvalvonta (access control) sekä kiistämättömyys (non-repudiation). Kaikki osa-alueet koskevat tietoa eri muodoissaan: tiedostoina (dokumentti, www-sivu, ohjelma), tiedonsiirtoina (internet-yhteys, sähköpostiviesti) tai koneen keskusmuistissa olevana bittien joukkona, jota prosessori parhaillaan käsittelee. (Järvinen 2002, 22-27.)

Tietojärjestelmien rakentamisessa on huomioitava inhimilliset virheet tietojen syöttämisessä sekä huolehdittava luottamuksellisuuden säilymisestä kun tietoja tulostetaan, siirretään tai tallennetaan. Kuviossa 3 on oivallisesti kuvattu tietoturvan luottamuksellisuuden, eheyden sekä käytettävyyden moninaisuutta. (Hakala & Vainio & Vuorinen 2006, 319.)



Kuvio 3. Ohjelmistosuunnittelussa huomioitavat riskitekijät (Hakala ym. 2006, 319.)

Tietoturvan kuusi perustavoitetta on helppo muistaa ja ymmärtää, mutta käytännössä vaikeita toteuttaa. (Järvinen 2002, 23.)

4.3.1 Eheys

Tiedon eheyden tarkoituksena on, että tiedot ja tiedostot ovat totuuden mukaisia eivätkä ne oikeudettomasti tai hallitsemattomasti muutu tai tuhoudu inhimillisen toiminnan, laitteisto- tai tietojärjestelmävian tms. seurauksena. (Paavilainen 1998, 10.)

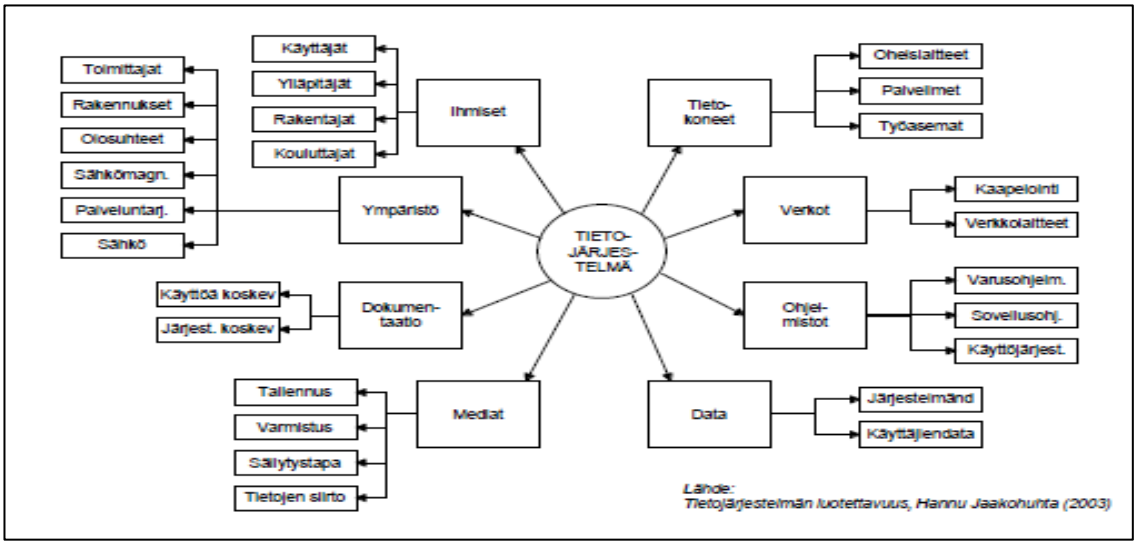
Eheyden turvaamiseen pyritään pääasiassa ohjelmistoteknisin ratkaisuin (esim. kryptaus). Sovelluksiin ohjelmoidaan erilaisia syöttörajoitteita tai syötteen tarkistuksia, tallennus- ja tiedonsiirto-operaatioihin varmistussummia tai tiivisteitä. Laitteistotasolla virheiden estämisessä käytetään esim. virheenkorjaavia muisteja tai väyliä. Tietoliikenneratkaisuissa käytetään sovittuja virheen tunnistus- ja korjausmekanismeilla varustettuja tiedonsiirron protokollia ja laitteita. (Hakala ym. 2006, 5.)

Tietojen määrän kasvusta ja tiedon monenlaisesta kopioitumisesta aiheutuu merkittäviä riskejä tiedon eheydelle.

4.3.2 Luottamuksellisuus

Luottamuksellisuudella varmistetaan, että tietojärjestelmän tiedot ovat vain niihin oikeutettujen henkilöiden tai tahojen käytettävissä eikä niitä paljasteta tai muutoin saateta sivullisten käyttöön. Tähän pyritään suojaamalla tietojärjestelmien laitteet ja tietovarastot käyttäjätunnuksin ja salasanoin. (Hakala ym. 2006, 4.)

Tietojärjestelmien luotettavuutta voidaan tarkastella monista eri näkökulmista. Kokonaisuuden hahmottamien on tärkeää. Tietojärjestelmä rakentuu joukosta erilaisia resursseja joiden toiminnan tulisi tukea organisaation tavoitteita. Kuviossa 4 on kuvattu tietojärjestelmän luotettavuuden kokonaisuus ja sen monia osa-alueita ja niihin liittyviä tekijöitä.



Kuvio 4. Tietojärjestelmän luotettavuuden kokonaisuus (Kangas 2010, jakso 4, 12.)

Luotettavuutta voidaan varmistaa mm. kattavalla testauksella sekä hyvällä dokumentoinnilla.

4.3.3 Käytettävyys

Käytettävyydellä (käytetään myös: saatavuus) varmistetaan se, että tietojärjestelmän tiedot ja niiden muodostamat palvelut ovat oikeutettujen käyttäjien käytettävissä oikeassa muodossa ja toiminnan kannalta etukäteen määritellyssä vasteajassa. (Hakala ym. 2006, 4.) Tiedon saatavuutta suojataan esimerkiksi hyvin suunnitelluilla varmistusmenettelyillä (mm. varmuuskopio), levyjärjestelmillä ja tietoliikenneverkon varalaitteilla. (Miettinen 2002, 129.)

Poikkeamatilanteisiin tulisi valmistautua etukäteen hahmottelemalla ennakoivasti tilanteita ja näiden pohjalta laatia jatkuvuussuunnitelma, joka sisältää toimenpideohjeet tilanteista toipumiseen.

4.3.4 Kiistämättömyys

Kiistämättömyys tarkoittaa tietojärjestelmän kykyä tunnistaa ja tallentaa luotettavasti tietojärjestelmän käyttäjän tiedot sekä tietojärjestelmässä tapahtuneet tapahtumat. (Hakala ym. 2006, 5.) Tietojärjestelmän tiedon käyttäjistä ja muutoksista muodostetaan lokitiedostoja.

4.3.5 Todentaminen

Todentaminen (autentikointi) tarkoittaa sitä, että käyttäjällä on tunnistamistiedon lisäksi jokin muu luotettava tapa (esim. salasana, sähköinen avainkortti, biometrinen tunnustus) todentaa oikeutuksensa käyttää tietojenkäsittelylaitetta tai tietojärjestelmää. (Miettinen 1999, 296.)

4.3.6 Pääsynvalvonta

Pääsynvalvonnalla tarkoitetaan niitä toimintoja ja menettelytapoja, joilla säädellään tietojärjestelmässä oleviin tietoihin pääsy vain todennetuille käyttäjille (henkilöt, sovellukset). (Hakala ym. 2006, 5.) Saman tiedon käsittelyyn voidaan määritellä henkilöille erilaiset käyttöoikeudet (esim. luku, muokkaus).

4.4 Tietoturvariskien hallinta

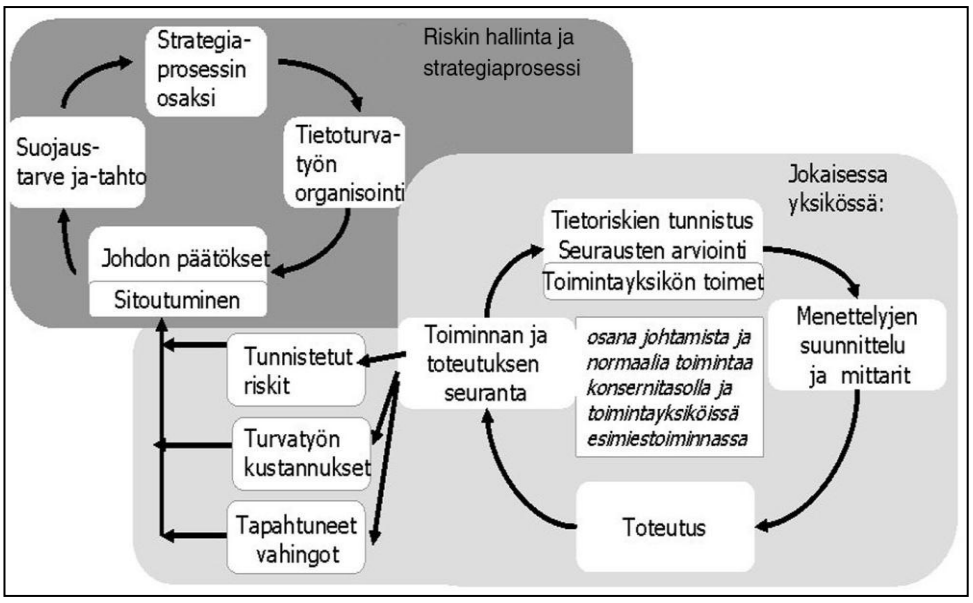
Tietoturvariskien hallinnalla suojaudutaan tietoriskeiltä. Tietoturvallisuuden oleellinen osa on liiketoiminnan prosessien tunteminen ja riskien tiedostaminen. Tietoriskit ovat muiden riskien tavoin mukana kaikissa liiketoiminnan prosesseissa.

Tietoturvallisuuden johtamisessa on käytännössä kyse riskienhallinnan toteuttamisesta. Päivittäisiin toimintaprosesseihin tulee sisältyä menetelmiä, joilla riskejä voidaan hallitusti vähentää tai niiden vaikutusta pienentää. Hyvin johdetussa organisaatiossa on määritelty selkeästi tietoturva- ja turvallisuustehtävät sekä niissä tehtävissä toimivien vastuut sekä heidän väliset raportointikäytännöt. (VAHTI 3/2007, 15.)

Tietoriskien hallinnassa voidaan erottaa tietosisältöön ja toimintatapoihin kohdistuvia riskejä sekä tietotekniikan ratkaisuihin ja hallintaan kohdistuvia riskejä (kuvio 5). (Teollisuusautomaation tietoturva 2005, 32.)

Kuvio 5. Tietoriskien hallinta liiketoiminnassa (Teollisuusautomaation tietoturva 2005, 32.)

Arkaluontoisten asioiden taitamaton käsittely voi vaikuttaa maineeseen ja luotettavuuteen toimijana. Yrityksen tietoturvan koordinoinnista ja johtamisesta vastaavan henkilön tulee olla ammatillisesti pätevä. Tietoturvahenkilöstön toimivaltuudet on oltava riittävät erilaisten tilanteiden käsittelyyn. Esimiesten osaamista tarvitaan tietoriskien arvioinneissa ja erityisesti häiriötilanteisiin luotavien toimintaohjeiden laatimisessa. Kuvio 6 kuvaa menettelyn, joka nivoo toimintayksikön menettelyt strategiaprosessiin ja johdon raportointiin. (Teollisuusautomaation tietoturva 2005, 32-33.)



Kuvio 6. Tietoriskien hallinnan strateginen ja operatiivinen taso (Teollisuusautomaation tietoturva 2005, 33.)

4.5 Lainsäädännön vaatimukset

Suomessa ei ole olemassa erityistä tietoturvaa koskevaa erillislakia, jossa olisi tyhjentävästi säädelty yhteisöjen tai yksittäisten tietokoneenkäyttäjien tietoturvavelvoitteista tai –oikeuksista. (Laaksonen ym. 2006, 21.)

Kotimainen ja kansainvälinen lainsäädäntö asettaa yrityksille ja muille yhteisöille suoria ja epäsuoria velvoitteita tietoturvallisuudesta huolehtimiseksi. Kun yrityksen tietoturvaa suunnitellaan, toteutetaan ja kehitetään, niin on otettava huomioon laissa määriteltyjä asioita. Vaatimusten määrään vaikuttaa toimiala ja liiketoiminnan luonne, joten yrityksen on ensin selvitettävä omaa toimintaansa ohjaavat säädökset. (Laaksonen ym. 2006, 18.)

5 Kehittämistehtävän viitekehys

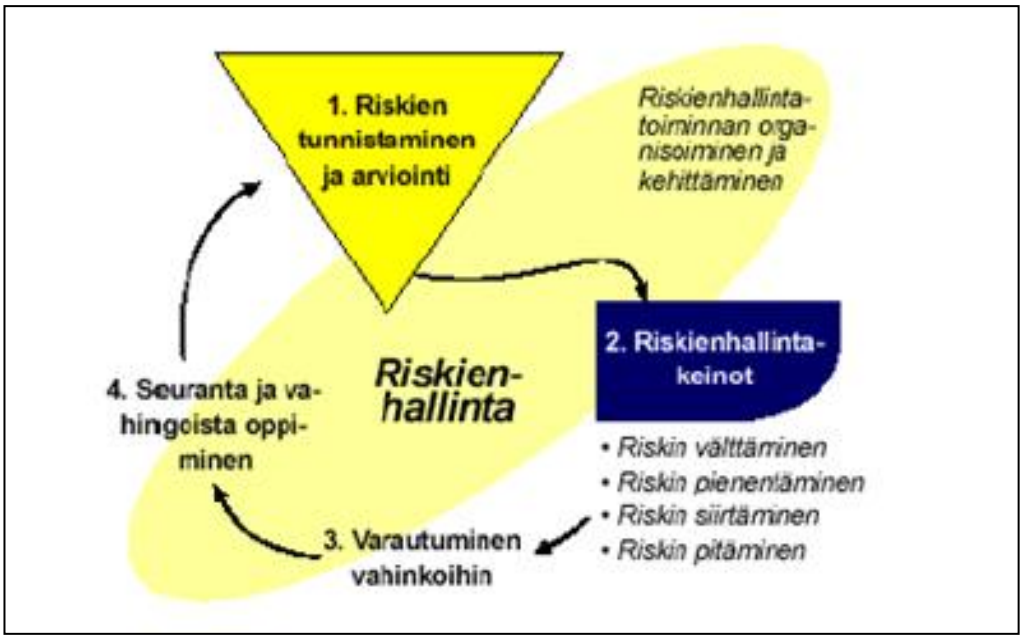
Tässä luvussa kuvataan kehittämistehtävän eri osa-alueiden tietoperustaa. Tietoperusta on valittu olemassa olevasta tiedosta, joka liittyy olennaisesti kehittämistehtävään.

Teoreettisen viitekehyksen materiaali muodostuu IT-riskienhallinnasta tietoturvan näkökulmasta sekä Kelan käyttämistä standardeista, VAHTI-ohjeista että COSO-ERM-mallista. Näistä materiaaleista saan selville kokonaisuuteen liittyviä osa-alueita, parhaita käytänteitä sekä niihin sisältyviä huomioitavia faktoja.

5.1 Riskienhallinta

Tietoturvallisuuden toteutumisen vaiheissa määritellään ensin suojattavat kohteet eli tiedot ja tietojärjestelmät, niiden arvo ja suojauksen arvo. Seuraavaksi arvioidaan uhkat ja riskit, jotka uhkaavat suojattavien tietojen turvallisuutta. Edellä mainittujen vaiheiden jälkeen voidaan valita sopivat kontrollit, joilla riskeihin varaudutaan, miten niiden toteutumisesta toivutaan ja ongelmat korjataan sekä miten toimintaa mitataan.

Riskienhallinta on tietoturvallisuuden tärkein osa ja se on suunnitelmallista ja jatkuvaa toimintaa. Tärkein sen tehtävistä on riskien pienentäminen eli riskin toteutumisen mahdollisuutta pienennetään hyväksyttävälle tasolle. Riski hallitaan poistamalla, pienentämällä, hyväksymällä tai siirtämällä se. Riskienhallintatoimet voidaan karkeasti jakaa omiin toimenpiteisiin ja riskin siirtämiseen (kuvio 7).



Kuvio 7. Riskienhallintaprosessin vaiheet (Mäkinen 2006, kalvo 39, alkuperäinen lähde http://www.pk-rh.com/startti-riskiehallintaan/mita-riskienhallinta-on/riskienhallintaprosessin-vaiheet.)

Teknologialla on kriittinen rooli riskienhallinnassa, mutta on huomioitava myös henkilöstö, toimintaprosessit, toimintatavat, organisaation rakenne ja toimintaympäristö, sekä lainsäädäntö.

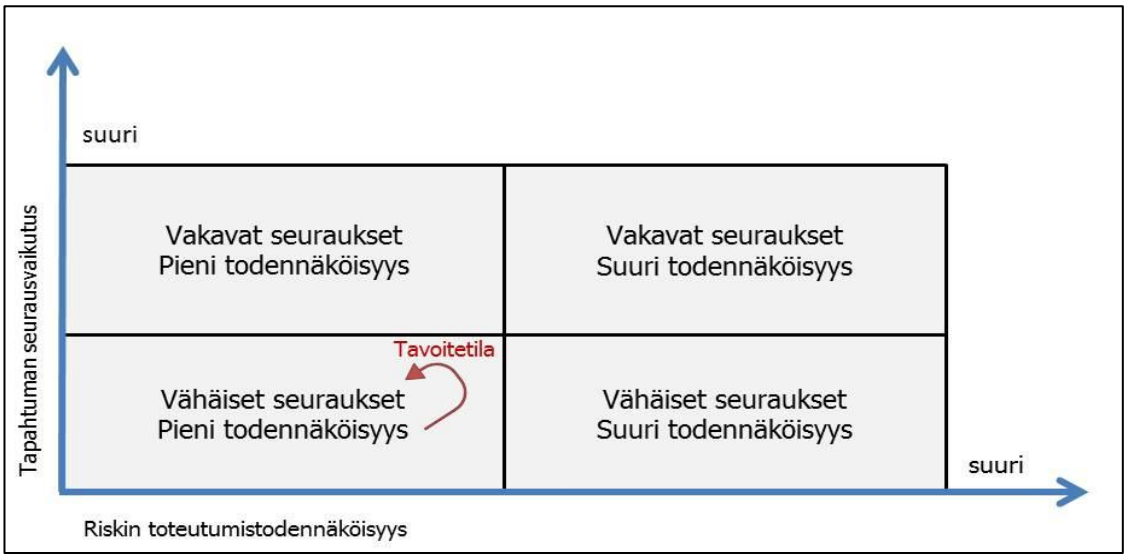
IT-riskien tunnistaminen tulisi olla osa sekä yrityksen kokonaisvaltaista riskienhallintajärjestelmää, että tietoturvallisuuden hallintajärjestelmää.

IT-riskien hallinnan edellytyksenä on, että organisaation toiminnan kannalta suojattavat kohteet on tunnistettu. Ensisijaiset kohteen IT-riskien näkökulmasta ovat liiketoimintaprosessit ja informaatio. Liiketoimintaprosesseista tulee tiedostaa niiden riippuvuudet IT-prosesseista ja tietojärjestelmistä. Informaation hallinnalla pyritään ymmärrykseen sitä mihin ja miksi tietoa tarvitaan ja mikä sen merkitys on. Suojattavia kohteita ovat laitteistot ohjelmistot, tietoverkko, toimitilat ja henkilöstö. IT-riskejä kannattaa luokitella organisaatioon sopeutettuna. Ohessa on lueteltu eräs tapa luokitteluun:

- Tietoriskit - vaarantavat tietoturvallisuutta

- IT-palveluiden tuottaminen, hankinta ja hallinta – vaarantavat IT-palveluiden tuottamisen ja johtamisen edellytyksiä. (Ilmonen & Kallio & Koskinen & Rajamäki 2010, 170.)

Tietoturvariskien merkittävyyttä voidaan tarkastella käyttämällä kuvion 8 mukaista nelikenttämallia. Pystyakseli kuvaa toteutuneen tietoturvariskin seurauksia ja vaaka-akseli kyseisen riskin toteutumisen todennäköisyyttä. Malli on jaettu neljään yhtä suureen lohkoon, joilla on tietyt ominaispiirteet. Kun tiedossa olevat tietoturvariskit sijoitetaan ao. lohkoihin, saadaan käsitys riskien suhteellisesta keskinäisestä tärkeydestä.



Kuvio 8. Tietoturvariskien hallinnan tavoitetila (Miettinen 1999, 60.)

Tietoturvariskien hallinnan tavoitetila asettuu kuvion 8 vasempaan alakulmaan. Tämän lohkonriskit ovat seurauksiltaan vähäisiä, ja niiden toteutuminen on epätodennäköistä. Kaikkien muiden lohkojen tietoturvariskit on pyrittävä saamaa tilaan, jossa ne lähestyvät koko ajan kuvion vasenta alakulmaa. Tietoturvariskejä voi havainnollisesti esittää myös laatimalla riskikartta. (Miettinen 1999, 58-60.)

Riskienhallintaan kuuluu oleellisesti raportointi joka voidaan jakaa ulkoiseen (esim. sidosryhmät, julkinen) ja sisäiseen raportointiin. Riskiraportointi ohjaa johtamista ja tukee ylintä - ja toimintayksiköiden johtoa päätösten teossa koskien operatiivista ja riskienhallintatoimintaa ja resursseja. Riskiraportointitapa ja ajankohta tulee määrittää. Riskiraporttien laajuus ja sisältö vaihtelee käyttötarkoituksen mukaan ja se on olennainen osa johdon raportointia. (Ilmonen ym. 2010, 187 ja 191.)

Kirjassaan Jordan ja Silcock (236-240) esittävät viisi järjestelmäriskien kehittymiseen vaikuttavia tekijöitä:

- Lisääntynyt riippuvuus tietotekniikasta
- Järjestelmien lisääntynyt monimutkaisuus (lisätään uusia ominaisuuksia tai esim. graafiset käyttöliittymät verrattuna tekstipohjaisiin)
- Järjestelmien erikoistuminen ja hajauttaminen yksittäisiin komponentteihin (esim. paketoidut ohjelmistotuotteet, järjestelmien monikerroksisuus, on-line- tai pilvipalvelut)
- Integrointi ja yhteensopivuus (esim. järjestelmien välinen rajapintojen määrä kasvaa niin myös mahdollisten integrointitapojen määrä kasvaa)
- Menneisyyden painolasti (huolellisesti tehdyt toiminnot vanhojen sovellusten poistossa silloin kun uusia on otettu käyttöön. Esim. päivitys- ja ylläpitotoimenpiteissä tulee huolellisesti päivittää samankaltaiset komponentit, jotta järjestelmien integriteetti varmistuisi).

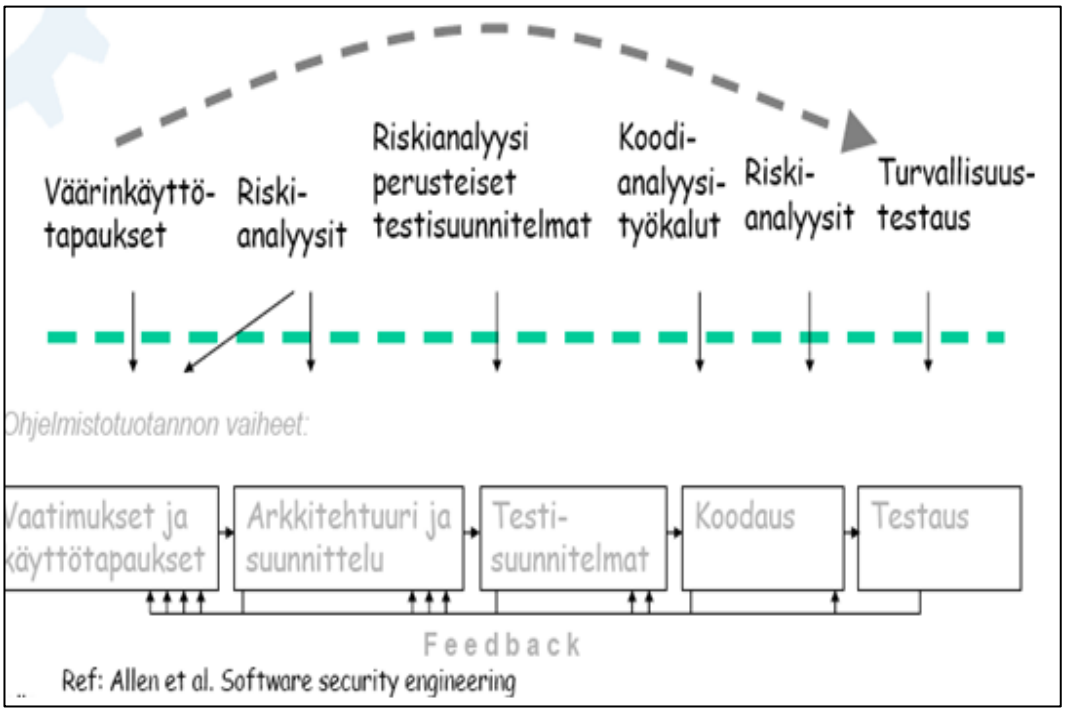
IT-riskien hallintakyky on tehokasta jos se täyttää liiketoiminnan tarpeet ja jossa on huomioitu seuraavat tärkeät seikat:

- Strategia ja käytännöt
- Strategioita ja käytäntöjä tarvitaan yleisten tavoitteiden määrittämiseksi, niiden yleisen tärkeyden ja priorisoinnin kiinnittämiseen, varmistamaan että IT-riskit on katettu asianmukaisesti sekä tarjota riskien arvioijille periaatteita, joiden varassa edetä.
- Roolit ja vastuut
- Roolit ja vastuut tulee sisällyttää työntekijöiden toimenkuvaan. Yhteiset vastuualueet on kohdennettava tarvittaessa, jotta varmistetaan se että kaikki osa-alueet on jonkun vastuulla.
- Prosessit ja lähestymistapa
- Luotettava IT-riskien hallintakyky perustuu sisäistettyihin ja johdonmukaisesti suoritettaviin prosesseihin.
- Henkilöstö ja sen pätevyys
- Henkilöstön tietotaitoja IT-riskien hallinnasta tulee kehittää ja ylläpitää. Koulutusta tulee antaa ko. käyttäjäryhmän roolille ja vastuualueelle sopivalla tavalla. (Jordan & Silcock 2006, 75-80.)

Poikkeusolot tai normaaliolojen häiriötilanteen saattavat vaikuttaa organisaation toimintaan lamauttavasti tai vaarantamalla keskeisten järjestelmien ja toiminnan turvallisuuden. Jatkuvuuden- ja poikkeustilanteiden hallinnan kautta organisaation on suunnitelmallisesti kyettävä varmistamaan toimintakykynsä. Painopisteenä tietoturvan suunnittelussa on tunnistaa uhat ja ennaltaehkäistä ne sekä välttämättömien toimintojen varmistaminen.

Jordan ja Silcock toteavat kirjassaan, että järjestelmät ovat riskialttiita riippumatta siitä onko järjestelmä uusi tai vanha, itse tuotettu tai ostettu, interaktiivinen tai suljettu. Sovelluksiin liittyvien riskien hallinta edellyttää järjestelmien ja sovelluksien elinkaaren sekä siihen liittyvien riskien ymmärtämistä.

Seuraavassa kuviossa (9) on havainnollisesti esitetty näkökulmaa tietoturvatehtäviin systeemityön eri vaiheissa. Sovellustietoturvassa on viisi kosketuspintaa (esim. vaatimukset ja käyttötapaukset) ja näkemyksiä tärkeimmistä tietoturvatehtävistä eri vaiheissa.

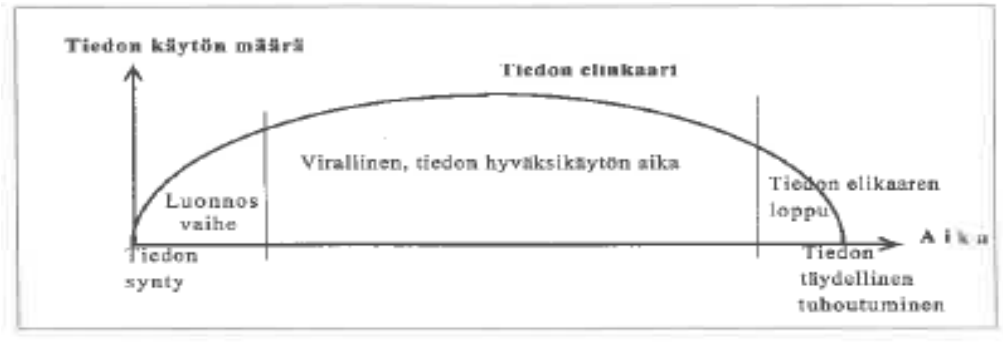


Kuvio 9. Ohjelmistojen turvallisuus eri vaiheissa (Brandt 2011, kalvo 146.)

Arkkitehtuuri ja suunnittelu vaiheessa arvioitavia asioita ovat mm. turvallinen toiminnallinen suunnittelu, hyökkäysten minimointi ja niistä toipuminen. Koodausvaiheessa teh-

dään koodianalyysiä (mm. syötetiedot, ylivuodot), määrällisiä analyysejä sekä huomioidaan hyvät ohjelmointikäytännöt ja testausvaiheessa käytetään mm. riskiperusteisia analyysimenetelmiä. (Brandt 2001, kalvo 147.)

Tiedon koko elinkaaren aikainen turvallisuustoiminta on vaikeasti hallinnoitava ja valvottava. Tietoturvariskit ovat suurimpia tiedon elinkaaren alussa eli luonnosvaiheessa ja tiedon käsittelyn elinkaaren lopussa (kuvio 10). Yleensä tiedon hyväksikäytön aikana tietoturva on hoidettu paremmin. (Paavilainen 1998, 29.)



Kuvio 10. Tiedon elinkaari (Paavilainen 1998, 29.)

Tietoa tulee suojata monella tavalla. Tiedon omistajan tulee tunnistaa suojaustarve. Tietojen käsittelyn laajuutta mietittäessä tulee tunnistaa mm. mitkä kaikki tiedot vaativat huolellista käsittelyä, missä olomuodoissa tietoja on sekä kuka tietää asioista. Tiedon luottamuksellisuus saattaa muuttua tiedon elinkaaren aikana. Tietoa tulee käsitellä liiketoiminnalle luokitellun arvon ja merkityksen mukaan sen käsittelyketjun kaikissa vaiheissa ja koko sen elinkaaren ajan. (Kyrölä 2001, 68-69.)

Tietoturvallisuuteen liittyvä riskienhallinta on osa organisaation kokonaisriskienhallintaa. Riskienhallintahallintapolitiikalla riskienhallinta kytketään osaksi johtamisjärjestelmää ja sen vuosittaista aikataulutusta. Riskienhallintapolitiikka on organisaation ylimmän johdon hyväksymä. Johto on myös määritellyt riskienhallinnan kattavuuden, vastuut ja sisäisen organisoinnin. Riskienhallintapolitiikalla jäsennetään hallinnan kokonaisuutta ja luodaan suuntaviivoja sen hoitamiseen ja kehittämiseen. (VAHTI 3/2007, 23-24.)

Yrityksen tietoriskejä hallitaan monella organisaatiotasolla. Johdon vastuulla on tunnistaa toimintaa uhkaavat sisäiset ja ulkoiset riskit, myös todelliset tietoriskit. Esimiehen

tulee hallita arkityössä tapahtuvat yllättävät tilanteet. Työntekijöiden on ymmärrettävä tiedon arvo omassa työssä. Teknisten asiantuntijoiden vastuulla on huolehtia tietoliikenneverkon toimivuudesta, laiteiden käytettävyydestä sekä sähköisen tiedon varmistamisesta. (Kyrölä 2001, 28-29.)

5.2 COSO-ERM -malli

Enterprise Risk Management – Integrated Framework (ns. COSO ERM) on kokonaisvaltainen riskienhallinnan malli (kehikko), jonka COSO-organisaatio julkaisi vuonna 2004. Kokonaisvaltaisen riskienhallinnan mallin tavoitteena on parantaa organisaatioiden sisäistä valvontaa, tunnistaa olennaisia kehittämistarpeita ja kehittää riskienhallintaprosessia kokonaisvaltaisesti. Riskienhallinnan mallissa määritellään toiminnan keskeiset käsitteet ja periaatteet ja kuvataan menetelmiä, joista on hyötyä mallin osa-alueita sovellettaessa. (Ilmonen ym. 2010, 32.)

Riskienhallinnan malli määrittelee riskienhallinnan prosessiksi, joka kattaa koko organisaation ja jota sovelletaan strategisten tavoitteiden mukaisesti kaikilla organisaation tasoilla. Malli on suositus, jota voi soveltaa organisaation omaan toimintaan sopivaksi.

Riskienhallinnan tavoitteena on tunnistaa potentiaalisia tapahtumia, jotka voivat vaikuttaa yrityksen toimintaan sekä hallita riskejä yrityksen riskinottohalukkuuden mukaisesti.

COSO ERM -mallissa yksi sivu rakentuu kahdeksasta toisiinsa kiinteästi yhteydessä olevista riskienhallinnan osa-alueista eli riskienhallintaprosessista. Osa-alueita ovat sisäinen toimintaympäristö, tavoitteenasettelu, tapahtumien tunnistaminen, riskien arviointi, riskeihin vastaaminen, valvontatoimenpiteet, tieto ja viestintä sekä seuranta erilaisten arviointien perusteella. (Ilmonen ym. 2010, 32.)

Riskienhallintaosa-alueet on COSO ERM -mallissa kuvattu suorassa suhteessa toisiinsa kolmiulotteisessa kuutiomatriisissa (kuvio 11).

Kuvio 11. COSO-ERM -mallin osatekijät (Sisäiset tarkastajat ry. 2004, 6.)

Ohessa on avattu mitä eri osa-alueet eli riskienhallintaprosessi sisältää.

- Sisäinen ympäristö

  Sisäinen ympäristö käsittää organisaation ilmapiirin ja henkilökunta tarkastelee ja käsittelee riskejä sen pohjalta. Henkilökunnan toimintaan vaikuttavat organisaation riskienhallintafilosofia, riskinottohalukkuus, rehellisyys, eettiset arvot sekä ympäristö, jossa arvoja sovelletaan.

- Tavoitteenasettelu

  Organisaation tavoitteiden tulee olla määritelty ennen kuin voidaan määrittää riskitekijöitä ja johto voi tunnistaa niiden toteutumiseen vaikuttavat potentiaaliset tapahtumat. Kokonaisvaltaisella riskienhallinnalla varmistetaan, että johdolla on käytettävissä prosessi tavoitteenasetteluun, että valitut tavoitteet ovat organisaation toiminta-ajatusta tukevia ja sen mukaisia ja, että ne ovat sopusoinnussa organisaation riskinottohalukkuuden kanssa.

- Tapahtumien tunnistaminen

  Organisaation tavoitteiden toteutumiseen vaikuttavat sisäiset ja ulkoiset tapahtumat tunnistetaan, ja samalla tehdään ero riskien ja mahdollisuuksien välillä. Mahdollisuudet kanavoidaan takaisin johdon tavoitteenasetteluun ja strategiatyöhön.

- Riskien arviointi

  Arvioidaan riskien mahdollisten riskitapahtumien vaikutusten laajuus organisaation tavoitteisiin. Riskit arvioidaan ottamalla huomioon niiden toteutumisen todennäköisyys ja vaikutukset, minkä pohjalta päätetään kuinka ne hallitaan.

- Riskeihin vastaaminen

  Organisaation johto päättää, kuinka strategisiin riskeihin vastataan. Muita riskienhallintapäätöksiä tehdään kaikilla organisaation tasoilla.

Riskit vältetään, hyväksytään, jaetaan tai niitä vähennetään. Johto laatii keinot riskien sopeuttamiseksi organisaation riskinsietohaluun ja riskinsietokykyyn.

- Valvontatoimenpiteet (päivittäisvalvonta ja tehtävien eriyttäminen)
  Laaditaan ja toteutetaan menettelytavat, joita käyttämällä riskeihin kyetään vastaamaan aiotulla tavalla.
- Tieto ja viestintä
  Tarvittava tieto tunnistetaan, poimitaan ja viestitään sellaisessa muodossa ja niin pian, että riskien vastaamistoimenpiteet voidaan toteuttaa ajoissa. Tehokas viestintä on sekä vertikaalista että horisontaalista.
- Seuranta
  Organisaation koko riskienhallintaa seurataan ja muutoksia tehdään tarpeen mukaan. Seurantaa suoritetaan sekä jatkuvan toiminnan että erillisillä, säännöllisillä arvioinneilla. (Sisäiset tarkastajat ry. 2004, 5.)

COSO ERM -mallissa tavoitteet on ryhmitelty neljään luokkaan: strategisiin, toiminnallisiin, raportointia koskeviin sekä vaatimustenmukaisiin. Strategisen tason tavoitteet luovat perustan toiminnalle ja niiden tarkoituksena on tukea toiminta-ajatusta tukevia ns. korkean tason tavoitteita. Toiminnalliset tavoitteet liittyvät organisaation voimavarojen tehokkaaseen ja taloudelliseen käyttöön. Raportoinnin tavoitteet tähtäävät siihen, että raportointi on luotettavaa. Vaatimustenmukaisuudella tarkoitetaan sitä, että toiminnassa noudatetaan sovellettavia lakeja ja määräyksiä.

Kolmas ulottuvuus COSO-ERM -mallissa on organisaatio. Riskienhallintaa toteutetaan organisaation kaikilla tasoilla ja kaikissa prosesseissa.

Kelan riskienhallinta pohjautuu COSO-ERM -malliin. Riskienhallintaprosessin tavoitteena on edistää Kelassa riskitietoisuutta ja riskien tehokasta hallintaa koko organisaation läpi sekä varmistaa, että johdolla ja hallituksella on riittävästi tietoa riskeistä päätöksentekonsa tueksi. Riskienhallintaprosessi on kiinteä osa johtamisjärjestelmää ja strategiaprosessia. Riskienhallinnan tehtävänä on varmistaa, etteivät Kelan hallittavissa olevat riskit vaaranna Kelan tavoitteiden toteutumista.

Riskienhallinnan tavoitteena on tunnistaa toimintaan vaikuttavat riskitekijät, arvioida riskit, suunnitella hallintatoimet ja varmistaa toiminnan riittävä laatu, jotta kulloinkin tarkasteltavalle toiminnalle, projektille tai prosessille asetetut tavoitteet voidaan kohtuulli-

sen varmasti saavuttaa. Riskienhallintaan kuuluvat sekä riskianalyysi (riskien tunnistaminen, arviointi ja hallintatoimet) että sisäisen valvonnan kokonaisuus.

5.3 Käytetyt standardit

Tietoturvallisuuden kehittämiseen ja hallinnoinnin avuksi on kehitetty suuri joukko erilaisia standardeja, viitekehyksiä ja toimintamalleja. Lisäksi tietoturvallisuuden eri osa-alueilla on omat juuri tätä kyseistä osa-aluetta käsittelevät standardit, jotka voivat olla luonteeltaan hyvinkin teknisiä. Keskeisimmät tietoturvastandardit ovat nykyisin ISO-standardeja. ISO-standardit ovat laajasti levinneitä ja tunnustettuja sekä kansainvälisesti hyväksyttyjä standardeja. ISO-standardit on pääsääntöisesti tarkoitettu ja suunniteltu yksityisen sektorin käyttöön, mutta ne soveltuvat hyvin myös julkisyhteisöjen käytettäväksi. (Laaksonen ym. 2006, 83-86.)

Kansainvälisiä standardeja on luotu tietoturvasuunnittelua varten. Niistä käytetään nimitystä ”tietoturvastandardi”, vaikka ne eivät asetakaan suoria vaatimuksia itse tietoturvalle (tasolle, sisällölle), vaan sen suunnitteluun. On hyvä muistaa se, että standardien noudattaminen ei sinällään takaa riittävää turvallisuutta. (Hakala ym. 2006, 46.)

Tietoturvan standardisoimisella pyritään yhteisten toimintatapojen laatimiseen ja sillä lisätään tuotteiden yhteensopivuutta ja turvallisuutta sekä helppokäyttöisyyttä. Standardeja käyttämällä voidaan osoittaa, että tietoturvallisuuden eri osa-alueet on käyty riskien kartoituksessa kattavasti läpi.

Standardit ja hyvät käytännöt auttavat jäsentämään tietoturvavaatimuksia sekä niiden todentamista. Vaatimusten ja turvatoimenpiteiden kohdistus vaatii tärkeiden toimintojen ja kohteiden tunnistamisen. Tärkeyttä voi arvioida esim. organisaation oman toiminnan, asiakkaiden, sidosryhmien tai yhteiskunnan näkökulmista. Toiminnan jatkuvuuden varmistamisen perusedellytys on tiedon käsittelyn turvaaminen. (Valtiohallinnon tietoturvatasot – esitutkimus, 2007, 8-9 ja 22.)

ISO/IEC 27000 -sarja on tietoturvallisuuden hallintaan suunnattu standardien kokoelma. Sarjan taustalla on British Standards Instituten BS 7799 -standardi, jonka ensimmäinen versio on vuodelta 1995. Vuonna 1999 standardi jaettiin kahteen osaan: Ensimmäisestä osasta muodostui ISO/IEC 17799 -standardi vuonna 2000 ja se uudelleen nimettiin standardiksi ISO/IEC 27002 vuonna 2005. BS 7799 -standardin toisesta osas-

ta muodostui ISO/IEC 27001 vuonna 2005. Ne eivät anna käytännön apuvälineitä tietoturvallisuuden integroimiseksi systeemityömalliin, mutta systeemityömallia kannattaa joka tapauksessa arvioida näiden standardien vaatimuksia vasten.

ISO/IEC 27001 -standardi määrittelee tietoturvallisuuden hallintajärjestelmän vaatimukset mahdollistaakseen riskien arvioinnin ja tarvittavien ehkäisevien toimenpiteiden toteuttamisen Standardi edellyttää paljon tietoturvallisuuteen vaikuttavien asioiden suunnittelua, kirjaamista ja dokumentointia toimenpiteiden toteuttamisen ohella. Perimmäisenä tarkoituksena on suojella luottamuksellisuutta, eheyttä ja saatavuutta (CIA-malli).

ISO 27002 -standardi on tietoturvallisuuden hallintaa koskeva menettelyohje, joka kuvaa tietoturvahallinnan tavoitteita ja hallintatoimenpiteitä. ISO/IEC 27002 -standardin toteuttamisohjeita ei käydä läpi, mutta niitä on tarpeen mukaan huomioitu lopputuloksessa.

Tietoturvastandardien tarkoituksena on opastaa organisaatioita parantamaan tietoturvaa ja varautumaan etukäteen tietoturvauhkiin.

Järjestelmänkehittämisvaiheiden tietoturvallisuustehtävien arvioinnissa olen huomioiden ISO/IEC 27001 -standardinvaatimuksia, joita on esitetty seuraavassa kappaleessa.

5.3.1 ISO/IEC 27001 Valvontatavoitteet ja turvamekanismit

Käsittelen tässä kappaleessa ISO/IEC 27001:2005 tietoturvallisuusstandardiin sisältyviä eri valvontatavoitteita ja niihin sisältyviä turvamekanismeja. Standardi jakaa tietoturvallisuuden 11 turvavalvontakohtaan ja kussakin niistä on 1-10 pääturvallisuuskategoriaa. Turvavalvontakohdat jakavat standardin toiminnallisiin osiin ja pääkategoriat määrittelevät tavoitteet tarkemmalla tasolla. Kuhunkin pääkategoriaan liittyy kohde ja siihen liittyviä kontrolleja, joilla määriteltyihin tavoitteisiin pyritään. Standardissa tarjotaan perussuuntaviivat ja siinä on kuvattuna vähimmäisvaatimuksina pidettävät kontrollit. Organisaation tulee miettiä lisää kontrolleja oman toiminnan näkökulmasta.

Oheisessa taulukossa (2) on esitelty standardin ryhmittelytapaa.

Taulukko 2. Malli ISO/IEC 27001 standardin ryhmittelyistä.

<table>
<tr><th colspan="3">A12 Tietojärjestelmien hankinta, kehitys ja ylläpito (turvavalvontakohta)</th></tr>
<tr><td colspan="3">A12.1 Tietojärjestelmien turvallisuusvaatimukset (pääkategoria)
Tavoite: Varmistaa, että tietojärjestelmät kehitetään turvallisiksi.</td></tr>
<tr><td rowspan="2">A12.1.1</td><td rowspan="2">Turvallisuusvaatimusten analyysi ja määrittely (kohde)</td><td>Turvamekanismi (kontrolli)</td></tr>
<tr><td>Uuden tai olemassa olevan jne.</td></tr>
</table>

ISO/IEC 27001 -standardissa prosessimainen toimintamalli perustuu PDCA-malliin (Plan-Do-Check-Act, suomenkielenvastine on - suunnittele, toteuta, arvioi, toimi), joka on organisaation johtamismalli toimintojen suunnitteluun, kehittämiseen ja ohjaukseen ja se sisältää menettelytavat tietoturvan osa-alueiden ohjaamiseen. Tietoturvan hallintajärjestelmän avulla pyritään takaamaan liiketoiminnan jatkuvuus sekä toisaalta minimoimaan tietoturvahäiriöitä ja niistä aiheutuvia seuraamuksia. Organisaation odotetaan noudattavan luotua tietoturvapolitiikkaa ja standardeja sekä teknisiä tarkastusmenetelmiä muun muassa tietojärjestelmille.

Tieto tulee luokitella organisaation määrittelemien luokitteluperiaatteiden mukaisesti riittävälle tasolle (A.7 Suojattavien kohteiden hallinta). (ISO/IEC 27001 2006, 34.)

Henkilöstöturvallisuuden yhtenä tavoitteena on se, että eri rooleilla toimivat käyttäjät ymmärtävät omat velvollisuutensa ja ovat tietoisia tietoturvallisuuteen liittyvistä uhkista ja niiden merkityksistä. Käyttäjille tulee järjestää asiaankuuluva koulutus heidän toimenkuvansa kannalta tarkoituksenmukaisella tavalla. (A8 Henkilöstöturvallisuus). (ISO/IEC 27001 2006, 36.)

Organisaation tietojärjestelmiä tulee käyttää asianmukaisesti ja tietoturvallisesti, jotta voidaan ehkäistä tietojen luvaton käyttö tai sen muuttuminen. Käytännön toimia on standardissa mainittu seuraavasti

- Menettelyohjeet tulee olla dokumentoituna, niitä on ylläpidettävä ja niiden tulee olla saatavilla sovitusti
- Tehtävät ja vastuualueet tulee olla eriytettynä
- Kehitettävät, testattavat ja tuotannossa olevat palvelut tulee olla toisistaan erotettuina

- Varmistetaan, että ulkopuolinen palveluntoimittaja noudattaa sopimustenmukaisia turvamekanismeja (A.10 Tietoliikenteen ja käyttötoimintojen hallinta). (ISO/IEC 27001 2006, 40.)

Uuden tietojärjestelmän käyttöönottoon, järjestelmiin tehtäviin päivityksiin ja uusien ohjelmaversioiden siirtoon pitää luoda hyväksyntäkriteerit ja riittävät testaukset. Muutostenhallinnan tulee olla valvottua ja muutosten turvallisuusvaikutukset on arvioitava. Käytöstä poistettavat tietovälineet tulee poistaa turvallisella ja varmalla tavalla. Kehityksen osalta vaaditaan, että testiaineistot on valittu huolellisesti, ja ne ovat suojattuja ja valvottuja (A.10 Tietoliikenteen ja käyttötoimintojen hallinta sekä A.12 Tietojärjestelmien hankinta, kehitys ja ylläpito). (ISO/IEC 27001 2006, 42 ja 52.)

Luvattomien tietojenkäsittelytoimintojen havaitsemiseen käytetään tapahtumalokeja. Lokeihin tallennetaan käyttäjien toiminta, poikkeamat ja tietoturvatapahtumat. Lokeja tulee säilyttää sovitusti. Häiriöt kirjataan ja analysoidaan ja tehdään tarvittavat toimenpiteet. Lokitiedot tulee suojata niin, ettei muuttamismahdollisuutta ole ja pääkäyttäjien toiminnot tulee olla kirjattuna (A.10 Tietoliikenteen ja käyttötoimintojen hallinta). (ISO/IEC 27001 2006, 44 ja 46.)

ISO/IEC 27001 -standardi vaatii, että pääsynvalvonnan toimintaperiaatteet ovat laadittu, dokumentoitu ja katselmoitu liiketoiminta- ja tietoturvallisuusvaatimusten mukaisesti. Käyttöoikeuksien hallinnalla varmistetaan valtuutetun käyttäjän pääsy (esim. peruskäyttäjä, pääkäyttäjä, tukihenkilö, sovellus) ja valvonnalla estetään luvaton pääsy tietojärjestelmiin. Käyttäjien käyttöoikeuksia tulee uudelleen arvioida sovitun menettelyjen mukaisesti (A.11 Pääsyoikeuksien valvonta). (ISO/IEC 27001 2006, 46 ja 48.)

Tietotojärjestelmien hankinnan, kehityksen ja ylläpidon vaiheissa tulee varmistaa se, että tietojärjestelmä kehitetään turvallisiksi huomioiden turvallisuusvaatimukset. Turvallisuusvaatimukset tulee yksilöidä ja hyväksyttää ennen tietojärjestelmien kehittämistä ja käyttöönottoa. Asianmukaisilla turvamekanismeilla varmistetaan tietojen oikea käsittely (A.12 Tietojärjestelmien hankinta, kehitys ja ylläpito). (ISO/IEC 27001 2006, 50.)

Tietoturvahäiriöiden hallinnan tarkoituksena on varmistaa, että tietojärjestelmissä olevista heikkouksista ja tietoturvatapahtumista viestitään ja siten korjaaviin toimenpiteisiin ryhdytään riittävän ajoissa. Organisaation tulee määritellä tietoturvahäiriöiden raportointiin liittyvät menettelytavat, ja näiden tulee koskea kaikkia sidosryhmiä. Tietoturva-

häiriöistä kerätään todistusaineistoa mahdollista jatkokäsittelyä varten lainsäädäntö ja asetukset huomioiden (A.13 Tietoturvahäiriöiden hallinta). (ISO/IEC 27001 2006, 52 ja 54.)

Liiketoiminnan jatkuvuudenhallinnan prosessin tavoitteena on kuvata menettelyt, joilla organisaatio varmistaa päivittäiset toimintonsa mm. tietojärjestelmien häiriöiden tai katkosten vaikutuksilta. Liiketoiminnan jatkuvuussuunnittelu edellyttää organisaatiolta jatkuvaa prosessia keskeyttävien tapahtumien analysointiin sekä riskien arviointiin ja niiden hallintaan. Organisaation tulee laatia ja ottaa käyttöön jatkuvuussuunnitelma. Jatkuvuussuunnitelma tulee testata ja päivittää (A.14 Liiketoiminnan jatkuvuuden hallinta). (ISO/IEC 27001 2006, 54.)

Organisaation tulee noudattaa kaikkien asiaankuuluvien lakien sekä asetusten, säännösten ja sopimusten velvoitteiden ja kaikkien turvallisuusvaatimusten vaatimuksia. Kuhunkin tietojärjestelmään kohdistuvat turvallisuusvaatimukset tulee määritellä selvästi (A.15 Vaatimustenmukaisuus). (ISO/IEC 27001 2006, 54.)

5.4 ISF

Information Security Forum (ISF) on kansainvälinen loppukäyttäjäorganisaatioiden yhteistyöjärjestö, joka kehittää jäsenistön kokemuksiin perustuvaa tietoturvastandardia (The Standard of Good Practice for Information Security). Standardi keskittyy hyvinkin pieniin osa-alueisiin ja antaa konkreettisia ratkaisumalleja (parhaat tietoturvakäytänteet). Koska ohjeet ovat kattavia ja käytännönläheisiä, niin standardi sopii pohjaksi tietojärjestelmien tietoturvaratkaisujen kehittämiselle.

Standardissa ongelmakohdat on jaettu seuraaviin osiin: tietoturvallisuuden hallinta, kriittiset liiketoimintasovellukset, tietojärjestelmäasennukset, tietoverkot sekä tietojärjestelmänkehitys. Oheiseen taulukkoon (3) on avattu kirjan ISF kirjan mukaisesti tietojärjestelmäkehittämisen osa-alueet ja niiden sisältöä. (ISF 2007, area SD1-6.)

Taulukko 3. Tietojärjestelmäkehittämisen osa-alueet.

Osa-alue	**Sisältöä**
Kehittämisen hallinta	Rooli ja vastuut, kehittämismalli, laadun varmistaminen, kehitysympäristö

Tietoturvallisuuden hallinta	Hallinta, tietoturvatietoisuus, tietoturvallisuuden auditointi
Liiketoimintavaatimukset	Tietoturvavaatimukset, luottamuksellisuus-, eheys- sekä, jatkuvuusvaatimukset, tietoturvallisuuden riskianalyysi
Suunnittelu ja toteutus	Tietojärjestelmän suunnittelu, sovelluskontrollit, yleiset tietoturvakontrollit, tuotteiden turvallisuus, toteutus
Testaus	Testausprosessi, hyväksyntätestaus
Käyttöönotto	Käyttöönottotestaus, asennusprosessi, jälkitarkastus

Standardista on poimittu konkreettisia aihioita lopputuotokseen.

5.5 VAHTI-ohjeet

Suomessa Valtiovarainministeriö (VM) ohjaa ja kehittää valtionhallinnon tietoturvallisuutta. Ohjeita kehittää VM:n asettama valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI). VAHTI-ohjeistus on kokoelma tietoturvallisuuden eri osa-alueet kattavia ohjeita, jotka on tarkoitettu pääasiassa julkishallinnon käyttöön, mutta ne soveltuvat suurelta osin myös yrityskäyttöön. Näiden ohjeistuksien tavoitteena on parantaa valtionhallinnon toimintojen luotettavuutta ja jatkuvuutta tietoturvallisuutta kehittämällä. Ohjeistukset ottavat huomioon myös Suomen lainsäädännön ja erityisesti viranomaisten tietojärjestelmien toiminnan. Ohjeissa on tarjolla tarkistuslistoja, joiden avulla voidaan tarkastella oman toiminnan tietoturvallisuuden tilaa. VAHTI-ohjeet ovat vapaasti saatavilla Valtionvarainministeriön kotisivuilta Internetistä (www.vm.fi).

6 Järjestelmäkehityksen tietoturvan lähtötilanteen selvittäminen

Tässä luvussa tarkastellaan käytettävissä olevia tietoturvallisuusperiaatteita ja -ohjeistuksia. Kirjattu materiaali on koostettu Kelan sisäisistä asiakirjoista.

Tietotekniikalla ja järjestelmiin sisältyvillä tiedoilla on tärkeä merkitys Kelan toiminnassa. Riippuvuus tietotekniikasta ja erilaisten tietokantojen ja -verkkojen toiminnasta kasvaa edelleen. Sähköisiä palveluita kehitetään lisää. Tämä kaikki velvoittaa ottamaan entistä korostetummin huomioon eri järjestelmien yhteensopivuutta ja tietoturvallisuutta.

Kansalaisten oikeusturvan toteutumisen, heille tarjottavien palveluiden ja tehtävissä onnistumisen edellytyksenä on tietojärjestelmien suojaus, häiriötön toiminta sekä talle-

tettujen tietojen luotettavuus, oikeellisuus, ristiriidattomuus, kattavuus, ajantasaisuus ja käyttökelpoisuus.

Järjestelmäkehityksen tietoturvallisuus koostuu tietojärjestelmän elinkaaren eri vaiheissa sovellettavista tietoturvallisuusperiaatteista ja suoritettavista tietoturvallisuustehtävistä. Järjestelmäkehityksessä tarkastellaan tietoturvallisuutta käytettävän systeemityömenetelmän vaihejakomallin puitteissa.

Kaikessa systeemityössä tulee noudattaa Kelan tietoturvallisuusperiaatteita ja -ohjeita. Tietosysteemien kehittämistyö tehdään vaiheittain ja useimmiten projektimuotoisesti. Joka vaiheessa tulee ottaa huomioon tietoturvallisuuden kolme peruselementtiä: luottamuksellisuus, eheys ja käytettävyys. Tietojen turvallisuudesta on huolehdittava manuaalisesti ja tietotekniikan avulla tapahtuvassa tiedon käsittelyssä, tiedon kaikissa olomuodoissa ja tiedon koko elinkaaren ajan.

6.1 Tietoturvallisuuden periaatteet Kelassa

Tietoturvallisuusperiaatteet ja –ohjeet sisältyvät Kelan tietoturvallisuuskäsikirjaan, joka on saatavissa intranetistä. Käsikirjaan sisältyvät Kelan tietoturvallisuusperiaatteet ja taustamuistion, jossa selvitetään tietoturvallisuuden merkitystä. Käsikirjassa on määritelty tietoturvallisuuden eri osa-alueille tavoitteet, vastuut ja periaatteet. Käsiteltyjä osa-alueita on yhteensä 17, joista yksi on tietojärjestelmäkehitys. Osa-alueisiin voi liittyä ohjeita tai linkkejä sisäisessä verkossa oleviin tarkentaviin ohjeisiin. Ohjeisto kattaa toiminnan keskeiset osa-alueet. Toimintaohjeet kuuluvat päivittäiseen toimintaan ja ne koskevat tavalla tai toisella jokaista henkilöä.

Tietoturvallisuuskäsikirjassa on määritelty vastuunjaot ja siihen kuuluvat vastuut ja velvollisuudet. Tietoturvapoikkeamien havaitsemisista on kirjattu kenelle ongelmat raportoidaan ja miten.

Kelan johtoryhmä käsittelee keskeiset tietoturvallisuusasiat. Pääjohtaja ja johtajat kukin omalla toimialallaan hyväksyvät merkittävät tietoturvallisuuden kehittämistoimenpiteet sekä vastaavat siitä, että tietoturvallisuuden kehittämiseen ja ylläpitoon on käytettävissä riittävät resurssit. Pääjohtaja ja tietohallinnosta vastaava johtaja hyväksyvät tietoturvallisuusperiaatteet ja päättävät tietoturvallisuuden periaatteellisista linjauksista. Tieto-

turvallisuuden toteutumista seurataan järjestelmällisesti ja johdolle raportoidaan säännöllisesti.

Jokainen kelalainen on velvollinen noudattamaan annettuja tietoturvaohjeita sekä raportoimaan havaitsemistaan tietoturvallisuusongelmista.

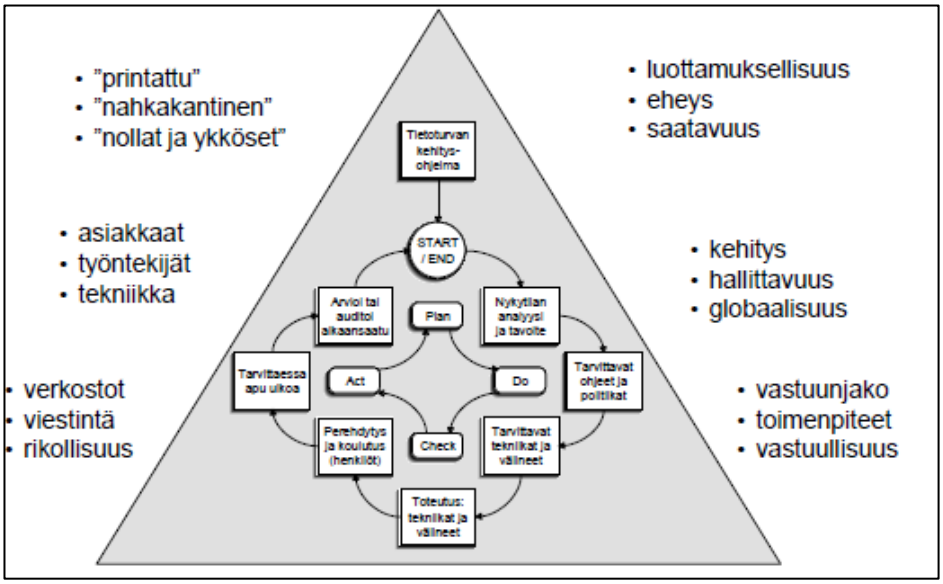
Toimihenkilöiden tietämystä ja osaamista tietoturvallisuudesta ylläpidetään kouluttamalla ja tiedottamalla.

7 Järjestelmäkehityksen tietoturvan tavoitetila

Tässä luvussa kuvataan tietoturvaa tietojärjestelmien kehittämisen näkökulmasta tietoturvan eri osatehtävissä Kelan iteratiivisessa systeemityömallissa. Kelan organisaatiossa tietoturvallisuuden hallinnassa korostuu arkaluontoisten tietojen käsittelyn turvaaminen lain mukaisesti.

Kelan nykypäiväinen toiminta on riippuvainen tietotekniikasta. Useat toimintaprosessit on suunniteltu tietotekniikan varaan ja vastaavien toimintojen toteuttaminen manuaalisesti voi olla mahdotonta tai liian kallista.

Tietoturvan kehittämisen prosessi on monisäikeinen. Tietoturvallisuuden kehittämisprosessissa käytäviä eri osatekijöitä on kuvattu kuviossa 12. Tehtäviä on jaoteltu avaamalla hallintajärjestelmää P-D-C-A.



Kuvio 12. Tietoturvallisuuden kehittäminen (Kangas 2010, jakso 1, 60.)

Kelan toiminta perustuu erilaisten tietojärjestelmien, tietoverkkojen, verkkopalveluiden käyttöön ja niiden luotettavaan toimintaan. Tästä syystä tietojärjestelmien tietoturvaan tulee kiinnittää huomiota jo niiden hankinnan tai rakentamisen alkuvaiheessa, esimerkiksi ottamalla huomioon järjestelmän tietoturvavaatimukset ja -uhkat mahdollisimman kattavasti.

Kelan tietojärjestelmiltä edellytetään suurta toimintavarmuutta. Sen turvaaminen merkitsee huomion jatkuvaa kiinnittämistä erilaisiin toiminnallisiin ja fyysisiin turvallisuuskysymyksiin, kehitysaskeleiden riskittömyyttä sekä sellaisten valmiuksien ylläpitämistä, joilla keskeiset maksusuoritukset asiakkaille voidaan hoitaa perille mahdollisimman pitkälle myös erilaisissa poikkeustilanteissa. Tietokantoihin kertyy huomattava määrä kansalaisia koskevaa arkaluontoista tietoa. Tämän vuoksi Kelan tulee varmistaa tietosuojajärjestelyjensä aukottomuus.

Kelan tietojenkäsittelyssä eletään isojen muutosten aikaa. Etuusjärjestelmien ja niitä tukevien tietotekniikkaratkaisujen ja –arkkitehtuurien kokonaisvaltainen ajanmukaistaminen on alkanut. Vuoden 2010 alussa käynnistyneessä etuusjärjestelmien uudistamishankkeessa uudistetaan kaikki Kelan 40 etuustietojärjestelmää sekä niiden noin 90 tukijärjestelmää teknisesti ja toiminnallisesti. Muutosten toteuttaminen kestää yli 10 vuotta. Kela siirtyy vähitellen PL1/CICS –ympäristöstä Java-ympäristöön.

Kelassa siirrytään uuden systeemityömenetelmän myötä vesiputousmallista iteratiiviseen systeemityömenetelmään. Iteratiivisena uusi menetelmä sopii perinteisiä menetelmiä paremmin oliopohjaisten järjestelmien tekemiseen. Systeemityömenetelmän tarkoituksena on varmistaa riittävä yhdenmukaisuus järjestelmäkehittämisessä ja edesauttaa näin työskentelyn hallittavuutta, tehokkuutta ja laatua. Kelan iteratiivinen systeemityömenetelmä perustuu IBM:n Rational Unified Process –menetelmistöön (RUP). RUP perustuu peräkkäisiin iteraatioihin, joista jokainen iteraatio suunnitellaan vesiputousmallin mukaisesti. Ideana on se, että projektin elinkaaren aikana työvaiheita toistetaan, iteroidaan, ja kunkin vaiheen lopuksi valmistuu osakokonaisuus, inkrementti, rakenteilla olevasta järjestelmästä. Kehittäminen jakautuu neljään vaiheeseen: aloitus, tarkennus, rakennus ja siirtymä. Unified Process ei ole itsenäinen prosessi vaan laajennettava kehys, jota muokataan vastaamaan organisaation tai projektin erityistarpei-

ta. Kelan Java-pohjaisten järjestelmien suunnitteluun ja toteutukseen on kehitetty systeemityömenetelmä, joka perustuu IBM:n RUPiin. Systeemityömenetelmä määrittelee, mitä tehtäviä pitää tehdä ja mitä lopputuotteita tuottaa missäkin vaiheessa projektia ja se tarjoaa yhtenäisen tavan työskennellä. Sivusto sisältää ja kuvaa myös roolit, työkalut, apuvälineet ja tukitoiminnot. Lisätietoa RUP-mallista on saatavilla mm. Internetistä eikä sitä käsitellä tässä kehittämistehtävässä tämän enempää.

Systeemityömenetelmän kehittämiseen liittyy aina turvallisuutta koskevia tekijöitä huolimatta siitä onko ohjelmat kehitetty organisaation sisällä vai hankittu ulkopuolelta.

Tutkimuksessa ei haeta uusia yksityiskohtaisia ohjeita tietoturvalliseen ohjelmointiin.

Tämän hetkinen systeemityömenetelmän käsikirja sisältää tietoturvaan liittyvänä dokumentin Tietoturvakysely. Uutta tietoturvallisuus sivustoa rakennetaan ja sinne kootaan mm. prosessia, suunnitelmamalleja sekä ohjeita.

8 Tutkimuksen tulokset

Tässä luvussa esitetään kehittämistyön tuottamat lopputulokset. Lopputuloksien valmistelussa suunnittelin ensin keskustelujen pohjaksi malleja, joita sitten työstettiin tai täydennettiin työpajoissa eteenpäin.

8.1 Kyselylomake

Kyselylomake menetelmällä saadaan kerättyä tietoa lyhyessäkin ajassa. Lomakkeen strukturoiduista kysymyksistä saadaan numeerista tietoa raportointiin.

Laadullisia aineistoja saadaan esimerkiksi haastattelemalla, havainnoimalla ja käyttämällä olemassa olevia dokumentteja. Määrällisiä aineistoja saadaan esimerkiksi kyselylomakkeella, suorittamalla mittauksia mittalaitteilla ja käyttämällä olemassa olevia tietokannoista löytyviä tietoja. Kyselylomakkeella voidaan määrällisten kysymysten ohella käyttää avoimia kysymyksiä, joiden vastaukset ovat laadullisia. Tehtävän kannalta tärkeintä on kyselyyn vastaavan joukon onnistunut valinta.

Tutkimuksen kyselylomake koostui kysymysten lisäksi taustakysymyksestä ja täyttöohjeista. Kyselylomakkeessa käytettiin sekä strukturoituja mielipidekysymyksiä että avoimia kysymyksiä. Mielipidekysymyksissä päädyttiin asenneasteikkojen käyttämiseen. Mielipidekysymysten tarkoituksena oli tutkia vastaajien mielipiteitä käytössä olevista tietoturvaohjeista. Avoimien kysymysten tarkoituksena oli kerätä ajatuksia ohjeistuksien kehittämiseksi.

Kyselylomakkeen laatimisessa haasteellista oli kysymysten oikeanlainen muotoilu, jotta vältettäisiin liian vaikeat tai sekavat kysymykset. Kyselylomake esitestattiin antamalla se luettavaksi yhdelle edustajalle. Saatujen kommenttien perusteella lomaketta muokattiin yksinkertaistamalla sekavilta vaikuttavia kysymyksiä ja selkeyttämällä vastausohjeita.

Kyselylomakkeen mukana lähetettiin saatekirje. Saatekirjeestä ilmeni kyselyn keskeiset asiat: tavoite, vastaajien valintaperuste, toteuttaja, kehittämistehtävän ohjaaja, ilmoitus tietojen luottamuksellisuudesta, vastaus aikataulu, palautusmenettely, kiitokset sekä yhteystiedot.

Ensimmäinen kyselylomake lähetettiin joulukuussa 2011 26 henkilölle sähköpostitse. Valitut henkilöt työskentelevät uuden systeemityömenetelmän eri vaiheissa ja erilaisilla rooleilla. Osallistujien valinnassa käytettiin edustavuutta, koska se vaikuttaa siihen, kuinka hyvin tulokset voidaan yleistää koko perusjoukkoa koskevaksi. Ensimmäisen kyselyn aikana uuden systeemityömenetelmän parissa työskenteli 50 henkilöä.

Ensimmäisen kyselyyn vastasi yhteensä 9 vastaajaa, joten vastausprosentiksi tuli n. 35 %. Jatkokysely lähetettiin maaliskuussa ja muistutuskyselyt kesä- ja lokakuussa 2013 ja niihin vastasi yhteensä 13 henkilöä, joten vastausprosentiksi tuli 50 %.

Kysymyksissä käytettiin asteikkoa 1-5. Asteikkojen arvot ovat seuraavat: 1= täysin eri mieltä, 2= osittain eri mieltä, 3= ei samaa mieltä eikä eri mieltä, 4= osittain samaa mieltä, 5= täysin samaa mieltä ja X= en osaa sanoa/en ole käyttänyt. Asteikon kohdalla on ensimmäisessä sarakkeessa ensimmäisen kyselyn tulokset ja vastaavasti toisessa sarakkeessa toisen kyselyn. Oheisessa taulukossa (4) on yhteenveto kyselylomakkeen strukturoitujen kysymysten vastauksista.

Taulukko 4. Kyselyiden 1 ja 2 yhteenvetotaulukko

Kysy sy-mys	Asteikko												Keskiarvo	
	1		2		3		4		5		X			
1			2	7	2	2	4	2			1	2	26/8 3,25	28/11 2,55
2				7	6	3	4	1			1	2	26/8 3,25	27/11 2,45
3		1	1	3	3	5	2	1			3	3	19/6 3,17	26/10 2,60
4	1	2	2	5	3	4	1		1		1	2	23/8 2,88	24/11 2,18
5		1	3	3	3	2	3	5				2	27/9 3,00	33/11 3,00
6		4	1	1	3	2	1	3	5	1		2	37/9 4,11	29/11 2,64
7		1	2	3	2	3	3	2	1		1	4	27/8 3,38	24/9 2,67

Ohessa on kirjattuna avointen kysymysten vastauksissa esille tulleita asioita ja aihioita.

Ensimmäisen kyselyn jälkeen:

1) Missä näet suurimmat haasteet uudessa systeemityömenetelmässä tietoturvan osalta?

- tietoturvaan liittyvien asioiden ja menetelmien tietoon saattaminen kaikille osapuolille
- konkreettisia tietoturvaselvityksiä
- jalkautus.

2) Millä tietoturva osa-alueella ja miten tulisi lisätä henkilöstön osaamista?

- katselmointia ja niihin yhteiset katselmointilomakkeet
- lokimenettelyt, laadunvarmistus, tekninen turvallisuus, uhkamallinnus, haavoittuvuustestaus
- tietoturvavaatimusten tunnistaminen.

3) Kun järjestelmää kehitetään, niin mikä on mielestäsi tärkein kehittämiskohde systeemityön tietoturvallisuudessa? Miten/Miksi?

- tietoturvavaatimukset projektin eri vaiheissa - kartoitus/koulutus
- tietoturvakatselmointien kehittäminen
- ulkopuolinen auditointi.

Toisen kyselyn jälkeen:

1) Missä näet suurimmat haasteet uudessa systeemityömenetelmässä tietoturvan osalta?

- laaditun dokumentin tiivistämistä
- yleisellä tasolla ei saa kiinni
- roolit ja vastuu ovat epäselviä
- vaatii strategisia linjauksia ja päätöksiä sekä selkeyttä tietoturvan kehittämisen vastuista
- jalkautus käytäntöön
- ymmärrys miksi jokin asia pitää tehdä
- liian massiivinen ja laaja ohjeistus joka voi hämärtää päämäärän
- vaikeasti ohjeistettava asia, koska vaatii laajaa näkemystä projektin työvaiheista, työskentelytavoista ja lopputuotteista.

2) Millä tietoturva osa-alueella ja miten tulisi lisätä henkilöstön osaamista?

- tietoturvavaatimusten tunnistamista ja tekninen turvallisuus
- varsinaisen tietoturvatestauksen toteuttamisen vastuu
- osaamista käyttäjähallintaan ja ehkä myös lokimenettelyyn
- ohjelmiston laadunvarmistukseen katselmointimenettelyn kehittäminen
- ohjeistusta työn tilaamiseen toiselta yksiköltä
- toimeksiantajalle ja määrittelijöille kohdennettua opastusta
- kunnollinen tietoturvakoulutus
- helposti löydettäviä ja helppokäyttöisiä tietoturvaohjeita
- yleistä tiedottamista siitä mitä tietoturva on ja miten se vaikuttaa jokapäiväisessä työssä.

3) Kun järjestelmää kehitetään, niin mikä on mielestäsi tärkein kehittämiskohde systeemityön tietoturvallisuudessa? Miten/Miksi?

- käyttöoikeudet
- tietoturvavaatimusten tunnistaminen
- vastuuttaminen projektin eri rooleissa toimiville ja heille riittävän osaamisen varmistaminen
- henkilökunnan tietämys tietoturvasta
- tärkeintä on asian sisäistäminen ja mieltäminen jokaisen systeemityövaiheen osa-alueeksi. Asioita pitää ajatella kokoajan uudestaan tuoreista näkökulmista

- yleisesti tietoturvan ja siihen liittyvien tehtävien ja osa-alueiden lisääminen systeemityömenetelmään.

Mitä pitäisi tulosten perusteella päätellä? Lopputuotteet eivät ole käyttäjille mieleen, niihin ei ollut aikaa paneutua vai vastattiinko yleisestikin. Tilaaja on ollut koko kehittämisvaiheen aikana tietoinen siitä millä tarkkuustasolla lopputuotetta ollaan laatimassa. Dokumentti ’Tietoturvatehtävät järjestelmänkehityksen eri elinkaarivaiheissa’ sekä kohdan 8.3 mukainen yhteenveto toimitettiin sähköpostitse eikä yhteistä asiasisällön läpikäyntitilaisuutta pidetty joka varmasti rokotti kokonaisuuden hahmottamista ja sisäistämistä. Yleensä Kelan kehittämistöihin valitaan useampi henkilö valmistelemaan tehtävää. Opinnäytetyössä ohjeistuksen toteuttamistyö on tehty opiskelijan toimesta ohjaajan tukiessa kokonaisuuden suuntaviivoja.

Tietoturvan tehtävät ovat osa järjestelmäkehityksen tehtäviä, mutta tavoite oli tuoda niitä erityisesti esille uuden systeemityömenetelmän mukaisesti jaoteltuina. Tarkalla jaottelulla halutaan varmistaa se, ettei mikään osio jää aiheetta pois. Tehtävät tulisi tulla mietintään tarpeeksi ajoissa. Projektien tehtäväkirjot ovat erilaisia ja tietoturvatehtäviä haettiin kattamaan niitä mahdollisimman monelta näkökulmalta. Nyt valmistunut yksinomaan tietoturvaan liittyvä ohjeistus on vasta avaus tietoturvatehtäviä koskevien ohjeistuksien kokonaisuudesta ja se ei yksistään kasvata tyytyväisyyttä joka näkyisi kasvuna vastausprosenteissa. Mittaristoon saadaan kuitenkin alkuarvoja, joita sitten seurataan vuosien saatossa. Uuden systeemityömallin mukaisten järjestelmien kehitystyöt ovat vasta alkumetreillä. Mielestäni on hienoa, että laaditun ohjeistuksen osalta ollaan mukana alkumetreistä lähtien eikä vasta silloin kun muutettavien järjestelmien toteutustahti moninkertaistuu.

Elinkaarivaiheen tehtäviä jaettiin sopiviin paloihin sillä näin ne tulevat esille. Useiden tehtävien osalta niiden edistäminen jatkuu seuraavassa vaiheessa. Tehtäviä voi projektin vastuuhenkilö niputtaa. Vastuuhenkilön tarkkaa nimeämistä ei tehty koska katsottiin, että erilaisissa toimeksiannoissa tehtäväroolit vaihtelevat. Tehtäviä näyttää olevan paljon mutta tavoitteena on saada erilaiset tehtäväosiot esille ja sitä kautta herää mietteitä siitä kuinka moninaisiin osatehtäviin sisältyy tietoturvatehtäviä.

Osa vastausten näkökulmista on käsitelty lopputuotteessa (katselmointi, tietoturvavaatimusten tunnistaminen). Tarvetta on kaiketi laatia yleisellä tasolla uusia muita ohjeita

tai laajentaa käytössä olevaan katselmointimenettelyyn tietoturvanäkökulmaa. Sama koskee tietoturvavaatimuksia koskevan ohjeistuksen laadintaa.

Muutosvastarintaa ei ollut vaan koettiin, että lisäohjeistusta tarvitaan, mutta sen esittämistavasta varmaan on eri näkemyksiä kullakin vastaajalla. Ohjeistus on tarkoitus sijoittaa käytössä olevaan systeemityömenetelmään josta tarvitsija löytää sen helposti ja ohjeista on aina oikea versio käytettävissä.

Vastausten perusteella osaamisen lisääntymisen tavoite ei vielä toteutunut tällä ajanjaksolla, mutta organisaatiota hyödyntävä tietämys kehittämiskohteesta kasvoi. Tavoite oli tehdä ohjeistus, jonka avulla saa helposti kokonaiskuvan ja toimintamenettely olisi sama kaikissa projekteissa ja siten saadaan tietoturvatason tehtävien tekemiseen varmistusta. Asian sisäistäminen varmaan vie yleisestikin aikaa mutta sitä varten yleisesti järjestetään mm. tietoiskuja vaikka eri teemoilla kerrallaan. Vähitellen ne muodostaisivat hyvän kokonaisuuden ja samanlaisen tavan toimia.

Kyselyn yhteenvedon jälkeen lopputuotetta käsitellään tietoturvapäällikön toimesta ja siihen tehdään esille tulevien muutostarpeiden mukaiset muutokset jotka sopivat tietoturvaprosessin sen hetkiseen toimintamalliin. Varsinainen jalkautus tehdään Kelan yleisten prosessien mukaisesti. Jalkauttamisen jälkeenkin on yleistä se, että ohjeet tulevat tutuksi vasta kun niitä itse käyttää projektissa Tämän tutkimuksen mukainen ohjeistus on siihen asti käytettävissä.

8.2 Tietoturvaprosessi tietojärjestelmien näkökulmasta

Prosessien kehittäminen liittyy organisaation suunnitteluun ja kehittämiseen ja sen perusteena ovat organisaation visiot, strategiat ja toimintaperiaatteet. Prosessikuvaukset ovat prosessien johtamisen, hallinnan ja parantamisen välineitä. Ne auttavat hallitsemaan kokonaisuuksia, jäsentämään prosesseja ja toimijoiden vastuita sekä löytämään toiminnan tehostamistarpeita. Prosessikuvauksia voidaan käyttää myös tehtäviin ja toimintaan perehdyttämisessä, koulutuksissa ja tietoturvan palveluiden kehittämistyön apuna. (JHS 152, 1.)

Prosesseja voidaan kuvata monella eri tasolla ja tasojen yksityiskohtaisuus vaihtelee. Valitun kuvauksen tulee välittää tarpeellinen ja olennainen informaatio. Prosessikuvasten ylin taso on prosessikartta ja se antaa yleisen kuvan toiminnasta ja esittää toimin-

not kokonaisuuksittain. Siinä kuvataan ydin- ja tukiprosessit, pelkistetty organisaatio ja toimintaympäristö. (JHS 152, 6-9.)

Kehittämistehtävän yhdeksi tavoitteeksi otettiin tietoturvaprosessin hahmottaminen ja sen kuvaaminen tietojärjestelmien näkökulmasta. Prosessikartta luo puitteet toimintatapojen yhdenmukaistamiselle, lisää tietämystä kokonaistoiminnasta ja sen eri vaiheiden yksityiskohdista. Tietoturvan hallinnan toimilla ylläpidetään organisaatiossa turvallisia tietojärjestelmiä. Tämän kokonaisuuden hallinnan hahmottamiseksi laadittiin tietoturvan 0-tason prosessikartta (liitteet 3 ja 4, ei julkinen).

Prosessikartan laadinnan pohjaksi haettiin koko Kelan prosessikartta, jotta kuvauksessa käytettäisiin yhtenäistä menettelyä ja kieltä. Suunnitteluvaiheessa haettiin tietoturvaan liittyvien ydinprosessien tunnustamiseen ja osakokonaisuuksien ryhmittelyyn tapoja ja valittiin prosessiin liittyvät muut osatekijät mm. asiakkaat ja ydinprosesseja tukevat tukiprosessit. Prosessin sisällöstä laadittiin asiakirja ”Tietoturvaprosessi tietojärjestelmien näkökulmasta”. Siinä kerrotaan mm. ydinprosessien sisältöä, eri roolien välisiä vastuita ja mittarit.

Laaditussa prosessikartassa on kuvattuna mm. tietoturvatoiminnan päätoiminnot, ympäristö (sidosryhmät, asiakkaat) sekä tukiprosessit. Prosessikartta kuvaa toiminnan elintärkeitä toimintoja ja se on hyvä apukeino auttaa henkilöitä ymmärtämään ao. kokonaisuutta ja kuvauksen avulla voidaan esitellä ulkopuolisille havainnollisesti ko. prosessin vaiheita. Prosessin eri vaiheita määriteltäessä tulee huomioida tarkoituksen mukainen prosessin käsittelytaso. Kaikissa yhteyksissä toimintaa ei tarvitse kuvata yksityiskohtaisella tasolla ellei se ole tarpeen jonkin toisen prosessin kannalta.

Tietoturvan ydinprosessien eri aliprosesseja voidaan tarvittaessa kuvata (esim. uimaratakaaviona) tarkemmin toisessa kehittämistyössä. Tarkennuksissa kuvausten yksityiskohtaisuus lisääntyy kuvaustasoittain. Kirjatuista tukiprosesseista on olemassa ko. prosessinomistajan omat kuvaukset joihin tukeudutaan ao. tehtävän osalta.

8.3 Tietoturvatehtävät systeemityön kehittämisvaiheessa

Tässä luvussa kuvataan uuteen systeemityömenetelmään sisällytettyjä tietoturvatehtäviä.

Tietoturvaan liittyvien eri tehtävien ja niiden lopputulosten kartoittamisessa käytettiin apuna mm. tietoturvan eri osa-alueita kattavia VAHTI julkaisujen ohjeita ja tarkistuslistoja sekä standardeja ISO 27001 ja ISF. Riskienhallinnasta valittiin sopivia näkökulmia. Tähän toimeksiantoon liittyvät aihiot valittiin ja muokattiin Kelan prosesseihin sopiviksi ja sijoitettiin elinkaarivaiheen tehtäviksi.

Järjestelmäkehityksen tietoturvatehtävien rakentamisessa on huomioitava kehitettävän järjestelmän tietoturvaominaisuudet, kehittämisprosessin tietoturva sekä itse toimijoiden tietoturvatietoisuus (mm. toteuttaja, testaaja). Uuden järjestelmän suunnittelussa tulee huomioida käytössä olevat tietoturvaratkaisut ja peilata onko tarvetta muuttaa nykyistä infraa. Kokonaisarkkitehtuurin eri näkökulmiin (tieto, toiminta, teknologia (integraatio, sovellus), ja järjestelmä) tulee sisällyttää tietoturvaratkaisut. Toiminta-arkkitehtuurin (ympäristö) ratkaisu vaikuttaa siihen miten tietoaineiston tietoturvallisuus toteutetaan. Tavoitteena on se, että tietoturvatehtävät muodostuvat kiinteäksi osaksi työtä.

Kehittämistyössä lopputuotoksena laaditussa taulukossa on esitetty karkea luettelo tietoturvatehtävistä ja -turvaamisen päätuloksista kehitettävän tietojärjestelmän eri elinkaarivaiheissa Kelassa. Työvaiheen kohdassa on esitetty käytettävissä olevat yleiset ohjeet ja huomioitavat tukiprosessit. Ao. vaiheessa käytössä oleva erillinen työväline kirjataan luetteloon sekä ko. vaiheeseen nimetty vastuuhenkilö(t).

Tietojärjestelmien kehitystyö koostuu joukosta ajallisesti toisiaan seuraavista vaiheista ja näissä vaiheissa suoritettavista toimenpiteistä. Tätä tietojärjestelmän kehittämiseen liittyvien vaiheiden joukkoa kutsutaan tietojärjestelmän elinkaareksi. Tietojärjestelmän elinkaareen kuuluvien vaiheiden kokoonpano vaihtelee hieman käsityksistä riippuen. (Pohjonen 2002, 26.)

Iteratiivisessa systeemityömenetelmässä systeemityön tehtäviä tehdään jo aikaisemmissa elinkaarivaiheissa kuin oli tehty vesiputousmalliin perustuvassa menetelmässä. Tehtävistä muodostetaan paketteja joita siirretään tuotantoon sovitusti. Tässä toimintamallissa regressiotestin merkitys korostuu, jotta saadaan varmistetuksi prosessin uusien pakettien toimivuus aikaisempaan nähden.

Eri elinkaarivaiheissa laaditaan erilaisia dokumentteja joita sitten tarkennetaan seuraavissa vaiheissa. Riittävä dokumentointi ja niiden jatkuva ylläpito on tietoturvallisuuden

edellytys. Oikea-aikaisen dokumentoinnin tärkeys korostuu ylläpitovaiheessa. Katselmointeja suoritetaan toimeksiannossa sovittujen kohteiden osalta.

Luettelo on viitteellinen, koska tietoturvatehtäviä tulee aina tarkastella ko. tietojärjestelmän toimeksiannon kautta. Jokaisen järjestelmän kehittämistehtävän kohdalla tulee aina kriittisesti arvioida juuri siihen kokonaisuuteen liittyvien tietoturvatehtävien kokonaisuutta ja tärkeyttä. Ohessa on esitetty pääpiirteissään mitä eri tehtäviä eri elinkaarivaiheeseen sisältyy. Tarkempi tietosisältö on kuvattu liitteessä 5 (ei julkinen).

8.3.1 Esiselvitys

Uusien tietojärjestelmien ja niihin perustuvien palvelujen tietoturvallisuuden ja laadun perusta luodaan järjestelmäkehityksen yhteydessä esiselvitysvaiheessa. Tietoturvallisuus on siten järjestelmäkehityksen keskeinen osa-alue jo alkuvaiheista lähtien. (VAHTI 3/2007, 34.)

Esiselvitysvaiheessa selvitetään toimeksiannon mukaisen tietojärjestelmän kehittämistarve ja ratkaisuvaihtoehdot. Päätuloksena on tietojärjestelmän kehittämisehdotus tavoitteineen, rajauksineen, perusteluineen ja investointilaskelmineen. Analysoinnissa huomioidaan liiketoiminnan näkökulma.

Tietoturvatavoitteet tulee kuljettaa järjestelmän kehitysprosessin läpi, jotta vaatimusten alkuperä ja jäljitettävyys voidaan tarvittaessa osoittaa. Tietoturvatavoitteet tulee katselmoida, sillä niiden lausumien perusteella tehdään päätös jatketaanko järjestelmäkehitystä kuvatulla tietoturvatasolla. Katselmoijina tulee olla myös asiantuntijoita, joilla on riittävä tietämys tietoturva-asioista, järjestelmäympäristöstä ja järjestelmän käyttötarkoituksesta.

Esiselvitysvaiheessa on tärkeää tunnistaa tietoturvavaatimukset ja priorisoida ne. Tunnistettujen tietoturvariskien käsittelemisen prosessi tulee olla tietoista ja sen tavoitteena on tunnistaa toimintaan vaikuttavat tekijät, kartoittaa ja arvioida riskit ja niiden todennäköisyys sekä toteutumisen vaikutukset, suunnitella ja toteuttaa vastaamistoimet ja varmistaa toiminnan riittävä laatu. Havaitut tietoturvariskit toimenpiteet priorisoidaan. Avainriskejä tulisi vielä arvioida Kelan kriittisiä toimintoja ja palveluita vasten.

Tunnistettujen tietoturvariskien ja toiminnallisuuden perusteella voidaan hankittavalle/toteutettavalle järjestelmälle määritellä turvallisuustaso, joka kuvaa järjestelmän kriittisyyttä tietyllä asteikolla. Kehitettävälle järjestelmälle asetettava tietoturvallisuuden taso saattaa määräytyä kokonaan tai osittain lainsäädännön perusteella.

Esiselvittelyvaiheessa mm. selvitetään säädökset jotka ohjaavat tai rajoittavat rakennetta ja toimintaa, tehdään tietoturva riskianalyysi, tunnistetaan vaadittava tietoturvataso, hahmotellaan käyttäjähallinnat ja nimetään tietoturva-asiantuntija sekä määritellään tietojärjestelmän ja tietojen omistajuus. Omistaja vastaa mm. tietojärjestelmän toiminnan oikeellisuudesta, lainmukaisuudesta, jatkuvuuden hallinnasta, käytön luottamuksellisuudesta sekä käytettävyydestä ja dokumentoinnin ajantasaisuudesta. Omistaja päättää mm. tietojärjestelmän sisällön kehittämisestä ja muutoksista sekä tietoturvaratkaisujen valinnasta. Nimetään tietoturva-asiantuntija tietoturvatehtävien koordinointiin.

Tietoturvavaatimukset tulee varmistaa huomioiden organisaation omat sovitut toimintamallit, laadittu riskianalyysi sekä toimintaan liittyvät lait ja säädökset yms.

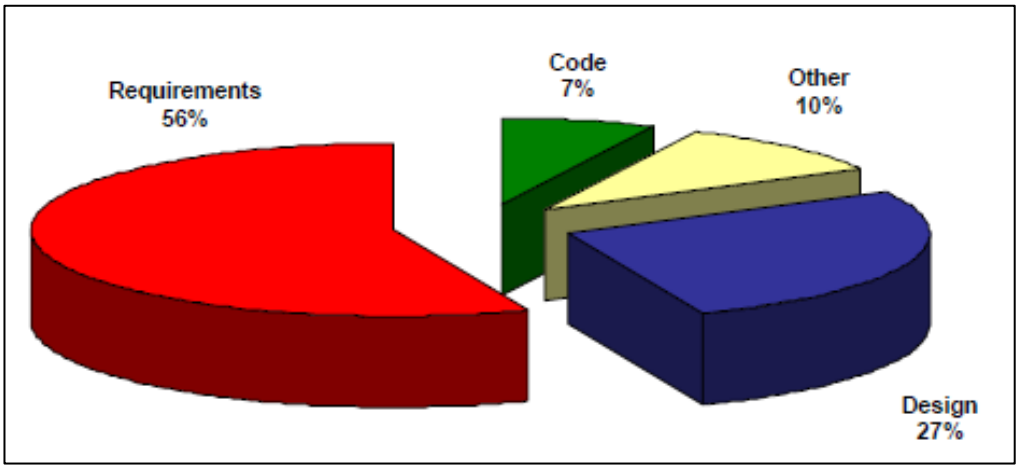
8.3.2 Määrittely

Määrittelyvaiheessa määritellään ja kuvataan toimeksiannon mukaisesti tietojärjestelmän yksityiskohtaiset vaatimukset, tieto- sekä toimintosisältö että rakenne. Etsitään järjestelmälle kriittiset käyttötapaukset.

Määrittelyvaiheen päättyessä tietoturvavaatimukset on kuvattu täsmällisesti/ yksityiskohtaisesti ja vaatimukset toteuttavat ratkaisut on määritelty. Valitaan järjestelmässä käyttöönotettavat suojaukset ja kontrollit.

Lopputuloksina ovat mm. määritelty käyttövaltuudet sekä jatkuvuus- ja toipumismenettely, laadittu alustava tietoturvatoimien testaussuunnitelma sekä suunniteltu arkistointimenettely. Kuvattu käyttötapaukset joissa on huomioitu poikkeustilanteiden käsittely. Kartoitettu integrointivaatimukset ja varmistettu se, että toimitaan kokonaisarkkitehtuurin mukaisesti.

Määrittelyvaihe on tietoturvasuunnittelun vaativin vaihe. Kaikista havaituista virheistä suurin % -arvo muodostuu vaatimuksista (requirements). Kuviossa 13 on esitetty jaottelua mistä virheet ja riskit ovat peräisin.



Kuvio 13. Virheiden ja riskien jakaumaa (Mäkinen 2006, kalvo 8. Alkuperäinen lähde James Martin, An Information Systems Manifesto.)

8.3.3 Suunnittelu

Suunnitteluvaiheessa suunnitellaan ja kuvataan toimeksiannon mukainen tietojärjestelmäratkaisu.

Suunnitteluvaiheen päättyessä järjestelmään sisällytettävät tietoturvaratkaisut on suunniteltu noudattaen tietoturvaperiaatteita. Tietoturvariskianalyysiä tarkennetaan teknisen suunnitelman tasolle. Tehdään arkkitehtuuritason ja toteutustyön suunnittelu.

Lopputuloksina ovat mm. päivitetyt tietoturvan riskianalyysi, toipumis- ja jatkuvuussuunnitelma sekä tietoturvatoimien testaussuunnitelma. Toipumissuunnitelmassa on kuvattu kriittisten ja tärkeiden toimintojen jatkaminen poikkeavissa tilanteissa. Tässä vaiheessa suunnitellaan myös sovittujen testi- ja tuotantoympäristöjen tietoturvamenettelyt sekä niissä käytettävät apuvälineet. Käyttäjien tarvitsema tietoturvaosaaminen on kartoitettu.

Suunnitteluvaihe luo perustan ylläpidolle, laajennuksille ja uusien ominaisuuksien käyttöönotolle. Tässä vaiheessa tulee tehdä oikeat ratkaisut haluttuun tietoturvallisuuden tasoon nähden. Suunnittelijan tulee tunnistaa toimintaympäristön riskit ja vaatimukset.

8.3.4 Toteutus

Toteutusvaiheessa tuotetaan sovitussa kehitysympäristössä suunnitelmien ja arkkitehtuurikuvausten mukainen tietojärjestelmä, järjestelmän osa tai muutokset olemassa olevaan järjestelmään huomioiden järjestelmälle asetetut vaatimukset.

Toteutusvaiheessa mm. konkretisoituu erityisesti virhetilanteiden käsittely- sekä lokimenettelyt.

Toteutusvaiheen päättyessä järjestelmään sisällytetyt tekniset tietoturvaominaisuudet on toteutettu mm. edellytetyt kontrollit ja käyttöoikeusmenettelyt. Toteutuksessa on noudatettu sovittuja ohjelmistoratkaisuja. Tietoturvakriittiset osiot on eriytetty. Tietoturvaominaisuudet on yksikkötestattu.

Lopputuloksina ovat mm. eri käyttäjäryhmille laaditut tietoturvatoimien käyttöohjeet ja asennussuunnitelmat sekä toteutettu säännösten mukainen arkistointimenettely.

Tietoturvalliseen ohjelmointiin liittyvien ohjeiden kartoittaminen tai laatiminen ei kuulunut tämän tutkimuksen piiriin.

8.3.5 Testaus

Testausvaiheessa varmistetaan vastaako tietojärjestelmä määriteltyjä (toiminnallisia, ei-toiminnallisia) tavoitteita ja vaatimuksia tai muita ominaisuuksia ja varmistetaan se että ratkaisut ovat toimivia ja hyväksyttäviä. Vaatimukset voivat olla joko käyttäjä- tai järjestelmävaatimuksia.

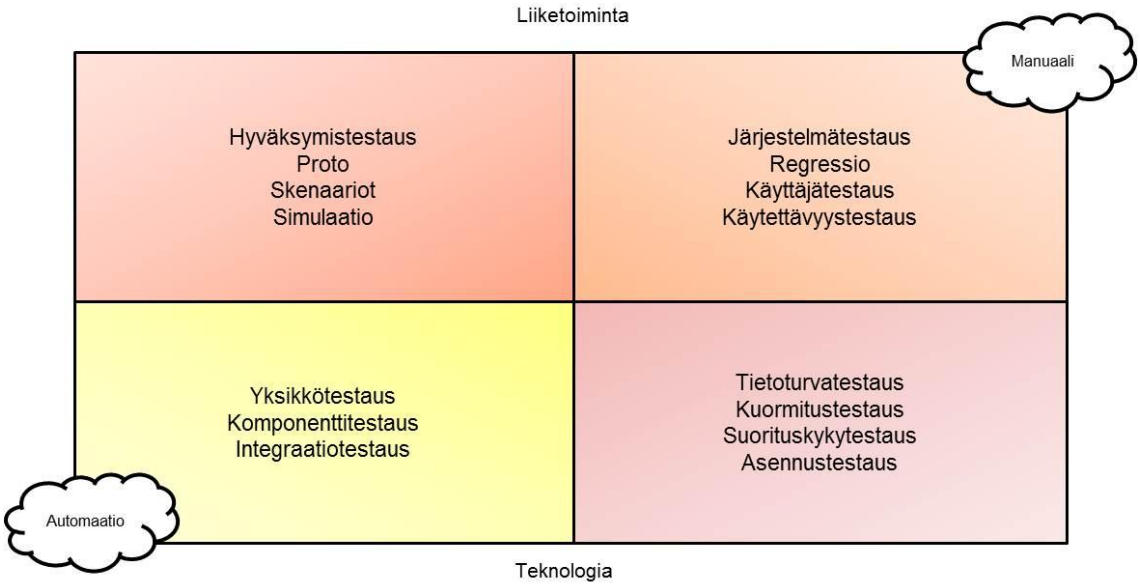
Tietoturvatestauksessa tavoitteena on löytää järjestelmästä mahdollisia tietoturva-aukkoja ja varmistaa järjestelmän toimivuus virhetilanteissa ja väärinkäytösyrityksissä. Testataan myös jatkuvuussuunnitelmaan kirjatut tehtävät.

Testausvaiheen päättyessä on varmistettu, että järjestelmään sisällytetyt tietoturvaominaisuudet on tehty ja ne toimivat tarkoituksenmukaisesti. Testaukseen on sisällytetty sekä normaalitilanteen että poikkeustilanteen mukaiset käsittelyt ja testausmenettely on dokumentoitu. Eri testausvaiheissa käytetään erillisiä testausympäristöjä ja testaus

suoritetaan testaussuunnitelmien mukaisesti. Testauksessa käytetään testiin soveltuvia apuvälineitä sopimuksen mukaisesti.

Tietoturvatehtävien varmistamisen sekä testauksien suorittamisen osapuolet on sovittu. Tarpeen mukaan käytetään ulkopuolisia auditoijia. Suunnitellaan eri käyttäjäryhmille sopivat tietoturvakoulutukset.

Tietojärjestelmän eri elinkaarivaiheissa suoritetaan erilaisia testauksia. Testaukset voidaan jakaa liiketoiminta ja teknologia lähtöisesti. Kuviossa 14 on hahmoteltu eri testausvaiheiden kirjoa joissa tietoturvatestauskin on osana tietojärjestelmän kokonaisuuden rakentamista.



Kuvio 14. Erilaisia testausvaiheita (mukaillen Seufert & Hassa 2010, kalvo 19.)

Järjestelmäkehityksen eri vaiheissa toteutetun suunnitelmallisen testaamisen avulla sovellusten tietoturvatasoa on mahdollista arvioida ja parantaa.

8.3.6 Käyttöönotto

Käyttöönottovaiheessa luodaan tietojärjestelmän todellinen käyttöympäristö tiloineen, laitteineen, tietokantoineen ja tietoverkkoineen määritysten mukaiseksi.

Ohjelmien asennuksien jälkeen on varmistettu tietojärjestelmän toimivuus, käytettävyys ja vaatimustenmukaisuus todellisessa tuotantoympäristössä. Käyttöönottovaiheessa toimitaan käyttöönottosuunnitelmien mukaisesti.

Lopputuloksina ovat mm. julkaistut käyttöohjeet, suunnitellut käyttövaiheen tietoturvajärjestelyt sekä ylläpitosuunnitelma.

Hyväksytyn käyttöönottovaiheen lopputuloksena on hyväksytty ja tuotantokäyttöön siirretty toimiva tietojärjestelmä, jonka tietoturvallisuus täyttää asetetut vaatimukset.

Käyttöönoton jälkeen järjestelmän toimintaa ja käyttöä seurataan sovitun käytännön mukaisesti ja tuloksista raportoidaan. Toipumissuunnitelman toimivuutta tarkastellaan ja testataan sovitusti.

8.4 Yhteenveto

Tietojärjestelmäkehityksessä tietoturvaan liittyvät tehtävät ovat moninaisia. Ohessa on kirjattu ylätasoisesti joitakin tietojärjestelmiin liittyviä riskienhallinnan paikkoja jotka tulisi olla hallinnassa järjestelmien koko elinkaaren aikana.

- IT-hallinnan prosessit on määritelty ja toimitaan tietyn prosessin/systeemityömenetelmän mukaisesti ja noudatetaan sovittuja ratkaisumenettelyjä (mm. standardit, ohjeet, hyvät käytännöt)
- Järjestelmien ja tietojen omistajuus on roolitettu sekä toimijoiden vastuut ja velvollisuudet on määritelty
- Pääsynhallinta ja käyttöoikeudet on suunniteltu kokonaisvaltaisesti ja tehtäviin sopeutettuna
- Tietoturvaan liittyvät tehtävät on määritelty ja vastuutettu
- On sovittu menettelyt seurantaan, valvontaan ja poikkeamista havaitsemisen raportoinnista (mm. lokitietojen käsittely)
- Testaukset on suoritettu eriytetyissä testausympäristöissä riittävän huolellisesti ja dokumentoitu
- Laadittu strategia, jossa on minimoitu häiriöiden vaikutukset ja mahdollistettu toimintojen uudelleen käynnistys (mm. jatkuvuussuunnitelma) ja varautumismenettelyiden toimivuus on testattu

- Käyttäjätuki on informoitu, heille on järjestetty tietoturvakoulutusta ja käytettävissä on tarvittavat käyttäjäohjeet
- Tarvittava tietoturvaosaaminen/tietoturvatietoisuus on varmistettu koulutuksilla ja sen ylläpidosta huolehditaan
- Ylläpidon, arkistoinnin ja käytöstä poiston toimintamenettelyt ovat jatkuvia ja suunnitelmallisia
- Kaikissa vaiheissa on huolehdittu riittävästä dokumentoinnista ja niissä on käytetty sovittua rakennetta. Niitä on katselmoitu sovitun menettelyn mukaisesti.

Tiedoista huolehtiminen kuvastaa yrityksen hyvää tietojenkäsittelytapaa. Sisäisten tietojen käsittelyyn liittyvä huolellisuus rakentuu tarkoituksenmukaisista työmenetelmistä, oikein toimivista ja luotettavista teknistä järjestelmistä sekä työympäristön suojaamisesta. (Kyrölä 2001, 23.)

Kokemuksen mukaan tietoriskein hallinnasta ainoastaan 20 % luodaan teknisillä ratkaisuilla, 80 % taataan työntekijöiden arkitoiminnan ja esimiesten johtamisen tuloksena. Tietoturvallisuuden tila kehittyy, kun ihmiset käsittelevät tietoja noudattaen luotuja toimintamenettelyjä ja käytäntöjä, kun järjestelmät ja ohjelmat käsittelevät tietoja oikein ja kun tiedot säilyvät oikeina. (Kyrölä 2001, 28-29.)

Tietoturvallisuuden kannalta henkilökunta voi osaamattomuudella, ymmärtämättömyyttään tai huolimattomalla käytöksellään aiheuttaa suurimpia tietoturvallisuuden ongelmia ja riskejä. Sen vuoksi tarvitaan tietoturvaperehdytystä, koulutusta sekä tietoturvatietoisuuden lisäämistä. Ohjeet ja niiden hallittu käyttöönotto tukevat tietoturvallista toimintaa käytännön työssä. Tietoturvassa on siis kyse tekniikasta ja työntekijöiden työskentelytavoista.

Siirryttäessä uuteen mallin niin kaikilla järjestelmäkehitykseen osallistuvilla henkilöillä on uutta opittavana. Uuden systeemityömallin mukaista työskentelytapaa tulee käyttämään suurin osa IT-projektien parissa työskentelevistä. Uusien tietoturvan ohjeistuksien tavoite on parantaa ja varmistaa tietoturvan näkökulman huomioiminen sopivassa laajuudessa ja oikeaan aikaan. Ohjeet ovat kiinteä osa tietojärjestelmäprojektin läpiviemistä. Ohjeita tulee päivittää esille tulleilla muutostarpeilla tai täysin uusilla vaatimuksilla.

Lähes kaikki tietoturvaa parantavat toimet ovat työntekijöiden kannalta ei-toivottuja, sillä ne vähentävät mukavuutta ja lisäävät työtä. Yrityksen tietoturvan edistämisessä tietoturvaohjeiden laatiminen on helpoin osa, mutta vaikeinta on saada ohjeet todella toimimaan myös käytännössä. Lopullinen tietoturva muodostaa ketjun, jossa on monta koneiden ja ihmisten muodostamaa lenkkiä, jossa lenkin pettäminen voi aiheuttaa harmillista uutisointia. (Järvinen 2002, 28 ja 111.)

Käytössä olevan ohjeistuksen toimivuutta ja tehokkuutta on voitava mitata jollakin järkevällä tavalla. Tämä on tärkeää, koska näin voidaan kehittää käytettävissä olevaa ohjeistusta edelleen ja löytää siitä mahdolliset puitteet, heikkoudet ja ristiriidat. (Miettinen 1999, 108.)

Uuden yksittäin tietoturvallisuutta tarkastelevan taulukon tavoitteena on helpottaa määrittelemään ja dokumentoimaan tietoturvavaatimuksia systeemityön eri vaiheissa ja pitkällä tähtäimellä turvata systeemityössä tasalaatuisuutta sekä yhtenäistämällä parantaa tietoturvallisuuden tavoitteiden toteutumista.

9 Johtopäätökset

9.1 Tutkimuksen pätevyyden arviointi

Tutkimuksen reliabilitetti (luotettavuus) toteutui, koska tutkimusaineisto ja tutkimuksen eri vaiheet on kuvattu sopivassa laajuudessa.
Toimintatutkimuksen raportista lukija saa yleiskuvan tietoturvan osa-alueista ja niihin kuuluvista teorioista. Kirjoitukset lopputuotteiden sisällöistä antaa käsityksen tapahtuneesta muutoksesta toimintamenettelyissä, vaikkei lopputuloksia ole saatavilla (salattu). Reliabiliteettia madaltaa se, että ensimmäisen kyselyn vastaajien lukumäärä jäi odotettua alhaisemmaksi ja siten odotetut toiveet ohjeistuksen sisältötarpeesta vähäisiksi.

Kehittämistehtävän liittyvät mittareita voidaan soveltaa kaikkiin tietoturvaan liittyviin tehtäviin eli mittarit ovat toistettavissa, eivätkä niissä mitattavat ominaisuudet muutu.

Kysymysten muotoilu oli onnistunutta. Vastaukset olivat rehellisiä ja realistisia. Toivoin enemmän konkreettisia toiveita ja täydennysaihioita liittyen juuri elinkaarivaiheisiin. Kyselylomake sopii käytettäväksi jatkossakin, kuten oli tavoiteltu.

Tutkimuksen validiteetti (pätevyys) toteutui, koska valituilla teorioilla saatiin luoduksi ratkaisu tutkimusongelmaan ja tavoitteisiin päästiin. Viitekehykseen valituista kokonaisuuksista sain muodostettua kokonaiskuvan ja valituksi aihioita lopputuloksiin.

Mittarit ovat selkeitä ja mittaavat niitä elementtejä, joita tutkimuksessa haluttiin mitata. Tutkimuksessa käytettiin laadullisia tutkimusmenetelmiä, raportoimalla ja dokumentoimalla riittävästi ja asianmukaisesti. Tutkimuksessa on lisäksi yhdistetty erilaisia tutkimusmenetelmiä sekä huomioitu tietoturvaan liittyviä erilaisia näkökulmia.

Tutkimuksen verifiointia (todentaminen) toteutettiin yhteistyössä tietoturva-asiantuntijoiden kanssa koko kehittämistyön rakentamisen aikana. Kehittämistyössä päästiin asetettuihin tavoitteisiin ja tutkimuskysymyksiin saatiin vastaukset.

9.2 Tutkimuksen suoritus

Valitun materiaalin avulla tutustuin viitekehysosassa esitettyihin tietoturvallisuuden standardeihin, ohjeisiin ja hyviin käytäntöihin. Tavoitteena oli löytää kehittämistehtävän tietoturvallisuuteen liittyvät aihealueet ja vaatimukset.

Valituista teorioista haettiin kohtia, joiden voidaan katsoa antavan tukea järjestelmäkehityshankkeen tietoturvallisuustehtävien läpivienteihin koko muutosaikajakson ajaksi. Ohjeistuksista sai suosituksia ja näkökohtia miten tietoturvavastuut jakautuu systeemityön vaiheissa eri rooleille.

Kehittämistyön tutkimusta suoritettiin henkilöhaastatteluin, tutustumalla nykyisiin dokumentaatioihin sekä kyselyllä. Tutkimuksen tulokset saatiin aikaan yhdistelemällä eri standardien, VAHTI-ohjeistuksien, opintomateriaalien sekä kirjallisuuden tietoja. Ohjaajan kanssa käytiin läpi erilaisia toteuttamistapoja, ideoita, näkemyksiä ja toteuttamaani materiaalia. Lopputulokset katselmoitettiin tietoturvatehtävien parissa työskentelevillä henkilöillä ja heiltä tuli vielä täydentäviä huomioita.

Lähteiden läpikäyminen vei aikaa. Lähteistä sopivien kokonaisuuksien ja niiden tietosisällön hahmottaminen organisaation tavoitteisiin oli vaativaa. Organisaatiossa tietoturva-asiat ovat jakautuneet usealle henkilölle. Heille on jaettu omat vastuualueet. Tässä keskityttiin haastattelemaan vain joitakin henkilöitä lähinnä Tietohallintoryhmästä ja IT-osastolta.

Työlle asetetut tavoitteet saavutettiin, koska kirjallisuuden, nykytilan tietojen ja haastatteluiden avulla saatiin tarvittava tieto Kelan tietoturvan liittyvän kehittämistehtävän pohjaksi. Uusien toimintatapojen sisäistäminen, siihen liittyvä opastusmenettely ja toimintatapojen soveltuvuuden seuranta ei valmistu kerralla vaan sitä tulee kehittää sovitun syklin mukaisesti. Organisaation kokonaisuuden osa-alueista tietoturva on kokoajan kehittyvä ja sen ajantasaisuutta on seurattava.

9.3 Vastaukset tutkimuskysymyksiin

1. Miten tietoturva liittyy tietojärjestelmäkehityksen eri elinkaarivaiheisiin ja millaisia tietoturvatehtäviä tunnistetaan?

Tietoturvatehtäviä tulee huomioida osana kaikkia elinkaarivaiheita. Tärkeätä on ottaa tehtävät huomioon riittävän ajoissa ja dokumentoida sovitun toimintatavan mukaisesti. Viitekehyksen materiaaleista löytyi raamit aihealueen kokonaisuuteen ja eri elinkaarivaiheiden tehtävien hahmottamiseen. Niistä pystyi koostamaan lopputuotetta. Eri elinkaarivaiheisiin tunnistettiin joko ao. vaiheeseen liittyviä tehtäviä tai tehtäviä jotka täydentyy kehittämistyön edetessä. Yhden tietoturvan tehtävän riville koostettiin omalle sarakkeelle ko. tietoturvatehtävän päätuloksia ja huomioitavia asioita. Ohjeistuksessa on kirjattujen tehtävien lisäksi kohdat ’Yleiset ohjeet’ ja ’Välineet’.

Eri elinkaarivaiheissa jaoteltujen eri osa-alueiden avulla toimija saa selkeän kuvan kokonaisuudesta. Toimii muistilistana ja tuo varmuutta siihen, ettei osa-alueita unohdu kokonaisuudesta. Vastuuhenkilö vastuuttaa eri tehtäväosien tehtävät ja seuraa toteutumista sovitun prosessin mukaisesti.

Ongelmana oli jaottelu iteratiivisen systeemityömenetelmän eri vaiheiden tehtäviin sopivaksi, löytää sopivia kokonaisuuksia, jotka aukeaisivat uudellekin toimijalle kertalukemisella sekä löytää sopiva taso tehtävän ja siihen liittyvien lopputulosten kuvaamiseen.

2. Mitkä tietoturvan osa-alueet on koettu ongelmallisiksi tietojärjestelmän kehittämisessä, joihin tarvitaan henkilöstön tietoturvatietämyksen lisäämistä järjestelmäkehityksessä?

Kyselyn vapaamuotoisesta osiosta saatiin ehdotuksia osa-alueista joita tulisi kehittää. Osaan vastauksista olisin toivonut enemmän lisätekstiä.

3. Miten käytännön tietoturvaohjeita tulisi kehittää vastaamaan paremmin käyttäjien tarpeita?

Kyselyn pohjalta saatiin tietoa erilaisista tietoturvaohjeiden kehittämistoiveista, joista tietoturvapäällikkö koostaa etenemissuunnitelman. Kysely lähetetään sovitun aikarytmin sisällä uudestaan, jotta uusia esille tulleita kohteita voitaisiin huomioida kehittämistehtäviksi. Tietoturvan arvioinnin laadullisiin ja määrällisin mittareihin saadaan historiatietoa ja nähdään muutosten suuntaa ja tarvetta painotuspisteisiin.

9.4 Jatkotoimenpiteet

Tietoturvallisuuden kokonaisuuden kehittäminen vaatii jatkuvaa ponnistelua ja uuden oppimista. Tässä kehittämistehtävässä toteutetut tulokset mielestäni ovat hyvä pohja kun suunnitellaan muita tarvittavia lisä- ja jatkotoimenpiteitä. Laadittua tietoturvatehtävien lopputulosta tulee päivittää käytön yhteydessä tulleiden kehittämistarpeiden mukaisesti. Kyselyn vapaamuotoisen osion teemat ovat tiedostetut ja niitä tulisi edistää.

Tärkeää oli saada laadittua tietoturvaan asiakirjoja osaksi jokapäiväistä työskentelyä ja siten se muodostuu käytännöksi. Toimintatapojen soveltuvuutta käytännön erilaissa projekteissa ja tilanteissa tulisi myös seurata. Pysyvät muutokset päivittäisessä toiminnassa selviävät vasta ajan myötä.

9.5 Itsearviointi

Tutkimusta työstäessäni sain tietoa tietoturvasta yleensä, siihen liittyvistä määritelmistä, toimenpiteistä ja eri osa-alueista lyhyesti sekä tietoturvan kehittämiseen liittyvistä haasteista. Alkuvaihe oli suunnittelua pidempi, sillä sopivan asiakokonaisuuden hah-

mottaminen ja asioiden sisäistäminen vei yllättävän paljon aikaa ja energiaa. Syvällinen käsitys tietoturvasta tulee vasta ko. tehtävien parissa työskennellessä. Tietoturvan kehittämisen suunnitteluvaiheissa oli myös tärkeää sisäistää tietoturvatehtävät organisaation omaan tietoturvatoimintaan. Tietoturva velvoittaa meitä toimimaan toimessamme. Aina sen osa-alueita ei näe tai hahmota konkreettisesti.

Toimintatutkimuksen laatimisen aikana selkenivät erilaiset yleiset käsitteet sekä tavat, joilla tietoturvaa voidaan jakaa osa-alueisiin. Toimintatutkimus osoittautui toimeksiantona hyvinkin mielenkiintoiseksi haasteeksi sen tärkeyden ja ajanmukaisuuden vuoksi. Vaikeutta tuotti työn sopiva rajaus siten, että sain laadituksi riittävän kattavan kuvan tietoturvaohjeistuksen kehittämiseen. Aihealueen käsittelemiseksi mietin pitkään ja tarkkaan sitä, kuinka työtä olisi asiallista lähteä kehittämään, jotta lopputulos hyödyntäisi organisaatiota. Orientoitumisprosessi oli pitkä ja haastava.

Oman osaamiseni kannalta sain lisäymmärrystä Kelan toiminnan tärkeästä osa-alueesta. Emme ole koskaan valmiita ja sen vuoksi oli hyväksi havaita, että aina oppii lisää. Työskentely tietoryhmäläisten kanssa edisti asioiden ymmärtämistä ja ryhmässä työskentelyn taitoja. Tutkimuksen tekeminen oman työn ohessa toi lisähaasteita.

Lähteet

Brandt, Harri 2011. TLTP-3110 Tietoturvallisuuden hallinta 3 op Syksy 2011.pdf-Http://www.pori.tut.fi/~braha/TTHallinta_syksy2011.pdf. Luettu 6.2.2013.

Hakala, Mika & Vainio, Mika & Vuorinen, Olli 2006. Tietoturvallisuuden käsikirja. WS Bookwell, Porvoo.

Huhanantti, Hellevi, Tietoturvallisuus tietojärjestelmän elinkaaren eri vaiheissa artikkeli. Sytyke ry –Systeemityö 3/98.

Ilmonen, Ilkka, & Kallio, Jani & Koskinen, Jani & Rajamäki, Markku 2010. Johda riskejä – käytännön opas yrityksen riskien hallintaan. Tammi, Saksa.

Information Security Forum (ISF) 2007. The Standard of Good Practice for Information Security.

ISO/IEC 27001:fi 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen standardisoimisliitto SFS, Helsinki.

JHS 152 Prosessien kuvaaminen. JUHTA- Julkisen hallinnon tietohallinnon neuvottelukunta. JHS-suositukset. 2008. Http://docs.jhs-suositukset.fi/jhs-suositukset/JHS152/JHS152.pdf 2008. Luettu 15.11.2011.

Jordan, Ernie & Silcock, Luke 2006. Strateginen IT-riskien hallinta. Edita Prima Oy, Helsinki.

Järvinen, Petteri 2002. Tietoturva & yksityisyys. WS Bookwell, Porvoo.

Kangas, Arto 2010. Liiketoiminta ja ICT-tarpeet. Luento, jakso 1. Metropolia Ammattikorkeakoulu, Vantaa.

Kangas, Arto 2010. ICT-avainteknologiat, arkkitehtuurit ja rakenteet. Luento, jakso 3. Metropolia Ammattikorkeakoulu, Vantaa.

Kangas, Arto 2010. ICT-hankinnat, isännöinti ja ylläpito tietoturvallisuus hankinnoissa. Luento, jakso 4. Metropolia Ammattikorkeakoulu, Vantaa.

Kyrölä, Tuija 2001. Esimies ja tietoriskien hallinta. WS Bookwell Oy, Juva.

Laaksonen, Mika & Nevasalo, Terho & Tomula, Karri 2006. Yrityksen tietoturvakäsikirja. Edita, Helsinki.

Loula, Pekka 2008. TLTP-3110 Tietoturvallisuuden hallinta, opintomateriaali. Http://www.pori.tut.fi/tdi/Tietoturvhall/TTHallinta2008Osa1.pdf. Luettu 1.9.2011.

Miettinen, Juha E 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Gummerus, Jyväskylä.

Mäkinen, Pekka 2006. Vaatimusten luomisesta kehitykseen ja testaukseen. International Merito Forum Oy / 09.05.2006. SoftQA Oy.
Http://www.softqa.fi/pdf/merito_20060509.pdf. Luettu 13.11.11.

Paavilainen, Juhani 1998. Tietoturva. Suomen Atk-kustannus Oy, Gummerus, Jyväskylä.

Pohjonen, Risto 2002. Tietojärjestelmien kehittäminen. Docendo Finland Oy, Jyväskylä.

Seufert, Christoph & Hassa Christian, Testing im Wandel, Behavious Driven Development & SpecFlow, TechTalk QM Frühstück 18. Februar 2010, Wien.
Http://www.techtalk.at/TechtalkWeb/media/Documents/Vortragsunterlagen/2010-02-18_BDD_Breakfast.pdf. Luettu 4.2.2013

Sisäiset tarkastajat ry. Enterprise Risk Management- Integrated Framework (Kokonaisvaltainen ajatusmalli organisaation riskienhallintaan). Tiivistelmä syyskuu 2004.

Teollisuusautomaation Tietoturva Verkottumisen riskit ja niiden hallinta. Suomen Automaatioseura ry Turvallisuusjaosto 2005, verkkopainos 2010.
Http://www.cert.fi/attachments/cip/5na1SblCp/SAS29_TeollisuusautomaationTietoturva.pdf. Luettu 4.2.2013.

Valtionhallinnon tietoturvatasot – esitutkimus, Hankeryhmän loppuraportti, 2007.
Http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070626Valtio/02_TTT_Loppuraportti_26062007.pdf. Luettu 5.7.2011.

Valtiovarainministeriö. 2003. Tietoturvallisuuden hallintajärjestelmän arviointisuositus. VAHTI 3/2003. Edita Prima Oy, Helsinki. Http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53808/name.jsp. Luettu 3.7.2011.

Valtiovarainministeriö 2003. Käyttäjän tietoturvaohje. VAHTI 5/2003.
Http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/51027/51024_fi.pdf. Luettu 15.2.2011.

Valtiovarainministeriö. 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. VAHTI 7/2003. Edita Prima Oy, Helsinki. Http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/name.jsp. Luettu 15.3.2011.

Valtiovarainministeriö. 2004. Tietoturvallisuus ja tulosohjaus. VAHTI 2/2004. Edita Prima Oy, Helsinki. Http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20040420Tietot/86049.pdf. Luettu 22.9.2011.

Valtiovarainministeriö 2004. Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. VAHTI 5/2004. Edita Prima Oy, Helsinki Http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/90727_fi.pdf. Luettu 4.2.2013.

Valtiovarainministeriö. 2006. Tietoturvatavoitteiden asettaminen ja mittaaminen. VAHTI6/2006. Edita Prima Oy, Helsinki. Http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060720Tietot/Vahti_6_06.pdf. Luettu 4.9.2011.

Valtiovarainministeriö. 2006. Tietoturvallisuuden arviointi valtionhallinnossa. VAHTI 8/2006. Edita Prima Oy, Helsinki. Http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060802Tietot/A_vahti_08_netti.pdf. Luettu 6.7.2011.

Valtiovarainministeriö. 2007. Tietoturvallisuudella tuloksia. VAHTI 3/2007. Edita Prima Oy, Helsinki. Http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071128Tietot/vahti3_07_netti.pdf. Luettu 17.2.2011.

Saatekirje

Kyselyn saatekirje nro 2 lähetettiin 28.3.2013

Hyvä kollega!

Sinut oli valittu osallistumaan tietoturvaan liittyvään kyselyyn, jossa kartoitettiin mitä ja miten tietoturvaohjeita tulisi kehittää käytettäessä uutta systeemityömenetelmää (James). Kyselyn kohderyhmään valittiin henkilöitä systeemityön eri elinkaarivaiheista, jotka ovat tällä hetkellä mukana kehittämisprojekteissa (Arkki).

Tietoturvallisuuden kehittäminen ja ylläpito on jatkuvaa toimintaa, joka tapahtuu hallinnollisten, fyysisten ja tietoteknisten ratkaisujen avulla. Tietojärjestelmien rakentamisessa tietoturvaa ei tule käsitellä erillisenä prosessina vaan osana eri elinkaarivaiheiden tehtäviä. Tietoturvatehtäviä tulee huomioida sovellusten rakentamisessa oikea-aikaisesti.

Kehittämistyön lopputuotoksena laaditussa taulukossa on luettelo tietoturvatehtävistä ja -turvaamisen päätuloksista kehitettävän tietojärjestelmän eri elinkaarivaiheissa Kelassa. Työvaiheen kohdassa on esitetty käytettävissä olevat yleiset ohjeet ja huomioitavat tukiprosessit. Ao. vaiheessa käytössä oleva erillinen työväline kirjataan luetteloon sekä ko. vaiheeseen nimetty vastuuhenkilö(t).

Eri elinkaarivaiheissa laaditaan erilaisia dokumentteja joita sitten tarkennetaan seuraavissa vaiheissa. Luettelo on viitteellinen, koska tietoturvatehtäviä tulee aina tarkastella ko. tietojärjestelmän toimeksiannon kautta. Jokaisen järjestelmän kehittämistehtävän kohdalla tulee aina kriittisesti arvioida juuri siihen kokonaisuuteen liittyvien tietoturvatehtävien kokonaisuutta ja tärkeyttä.

Tehtävien luokittelu varmistaa yhtenäisen toimintatavan ja lisää sovellusten yhteensopivuutta sekä turvallisuutta. Taulukon käytön avulla halutaan varmistaa se, että tietoturvallisuuden eri osa-alueita käydään ko. projektissa läpi.
Mahdollisuuksien mukaan läpikäy lomakkeen kokonaisuus. Käytä lomaketta siihen elinkaarivaiheen tehtävään jota olet nyt tekemässä ja tarkastele ko. vaiheen tietoturvatehtäviä.

Tutkimuksessa ei haettu uusia yksityiskohtaisia ohjeita tietoturvalliseen ohjelmointiin.

Luottamuksellisuus

Vastaukset käsitellään nimettöminä ja ehdottoman luottamuksellisesti, eikä yksittäisen henkilön vastaukset erotu analysoidusta aineistosta.

Kyselylomakkeen täyttäminen ja palauttaminen

Kyselylomakkeen sisältö on sama kuin ensimmäisessä kyselyssä. Tässä vaiheessa on valmistunut yksi tietoturvaan liittyvä ohje.

Kyselylomakkeen kysymykset ovat joko mielipide- tai avoimia kysymyksiä. Mielipidekysymyksiin vastataan ympyröimällä vaihtoehto (yksi vaihtoehto), joka vastaa parhaiten sinun henkilökohtaista mielipidettäsi tai kirjoittamalla avoimiin kysymyksiin vastaus ao. kohtaan.

Tavoitteen saavuttamisen kannalta jokainen vastaus on erittäin tärkeä.

Palauta oheinen kyselylomake täytettynä suljetussa kirjekuoressa pe 26.4.2013 mennessä minulle sisäisessä postissa. Vastaan mielelläni tutkimusta koskeviin kysymyksiin.

Kiitos jo etukäteen antamistasi arvokkaista vastauksista!

Tutkimusterveisin

Oili Koivuharju

Kyselylomake

Oheiset kysymykset liittyvät JAMES -systeemityömenetelmään ja näkökulmana ovat tietoturvan ohjeistukset järjestelmän kehitysprojekteissa.

Taustatiedot

Ympyröi toimenkuvaasi vastaava rooli: 1 = toimeksiantaja, 2 = määrittelijä, 3 = suunnittelija, 4 = toteuttaja tai 5 = testaaja.

Osa 1/Mielipidekysymykset

Ympyröi kysymyksen kohdalla omaa näkemystäsi parhaiten vastaava yksi vaihtoehto.

Ota kantaa kuhunkin väittämään ja käytä asteikkoa 1-5 seuraavasti: 1 = täysin eri mieltä ja 5 = täysin samaa mieltä. X = en osaa sanoa/en ole käyttänyt.

Nro	Kysymys	Asteikko					
1	Tietoturvaohjeista löydän tarvitsemani tiedon nopeasti.	1	2	3	4	5	X
2	Tietoturvaohjeita on helppo soveltaa.	1	2	3	4	5	X
3	Tietoturvaohjeet ovat riittävän ajan tasalla työtehtävieni kannalta.	1	2	3	4	5	X
4	Tietoturvaohjeet tukevat kattavasti työtehtävissäni.	1	2	3	4	5	X
5	Tietoturvaohjeiden noudattamiseksi minulla on tarvittava tietämys.	1	2	3	4	5	X
6	Tiedän keneltä saan tukea ohjeisiin liittyvissä lisäkysymyksissä.	1	2	3	4	5	X
7	Olen tyytyväinen saamaani tukeen.	1	2	3	4	5	X

Jos haluat, voit esittää perustelusi valinnalle.

Osa 2/Avoimet kysymykset

Kehitysideat kysymyksillä haemme tukeasi ja ideoitasi tietoturvatietoisuuden parantamiseksi järjestelmän kehittämisessä.

1) Missä näet suurimmat haasteet JAMES- systeemityömenetelmässä tietoturvan osalta?

2) Millä tietoturvan osa-alueella ja miten tulisi lisätä henkilöstön osaamista?

Esimerkkinä tietoturvallisuuden osa-alueista ovat mm. ohjelmistoturvallisuus (mm. ohjelmistojen ja tietokantojen pääsynvalvonta- ja varmistusmenettelyt, käyttäjähallinta ja sen valvonta, lokimenettelyt, ohjelmistojen laadunvarmistus (katselmointi), tekninen turvallisuus (mm. palvelujen ja palvelinten koventaminen, haavoittuvuustestaus) sekä tietoturvavaatimusten tunnistaminen (mm. sovelluksen tietosisällön mukainen luokittelu, -taso, uhkamallinnus).

3) Kun järjestelmään kehitetään, niin mikä on mielestäsi tärkein kehittämiskohde systeemityön tietoturvallisuudessa? Miten/Miksi?

Kiitokset osallistumisestasi kyselyyn.

Tietoturvaprosessi tietojärjestelmien näkökulmasta

Liite on salainen organisaation tietoturvallisuuden vuoksi.

Tietoturvaprosessin seliteteksti

Liite on salainen organisaation tietoturvallisuuden vuoksi.

Tietoturvatehtävät

Liite ovat salainen organisaation tietoturvallisuuden vuoksi.